An efficient key recovery attack on SIDH

EUROCRYPT 2023, LYON

Wouter Castryck & Thomas Decru

imec-COSIC,
KU Leuven, België

April 25th, 2023

Supersingular Isogeny Diffie–Hellman

- SIDH °2011 (Jao & De Feo)
- Previous security:
  - generic attacks with complexity $\mathcal{O}(\sqrt[4]{p})$ classical and $\mathcal{O}(\sqrt[6]{p})$ quantum (claw finding);
  - attack on unbalanced parameters (de Quehen, Kutas, Leonardi, Martindale, Panny, Petit, Stange);
  - chosen ciphertext attack against static key SIDH (Galbraith, Petit, Shani, Ti).

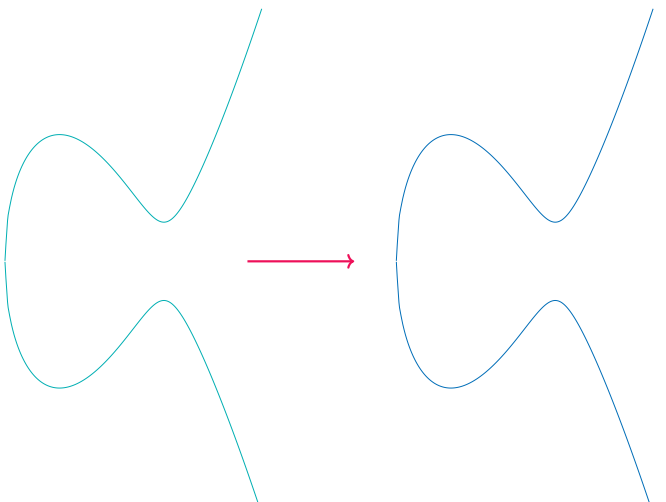
Supersingular Isogeny Diffie–Hellman

- SIDH °2011 (Jao & De Feo)
- Previous security:
  - generic attacks with complexity $\mathcal{O}(\sqrt[4]{p})$ classical and $\mathcal{O}(\sqrt[6]{p})$ quantum (claw finding);
  - attack on unbalanced parameters (de Quehen, Kutas, Leonardi, Martindale, Panny, Petit, Stange);
  - chosen ciphertext attack against static key SIDH (Galbraith, Petit, Shani, Ti).
- SIKE (Supersingular Isogeny Key Encapsulation) allows long term public keys.
- July 5th 2022: SIKE advances to Round 4 in NIST's post-quantum standardization process.

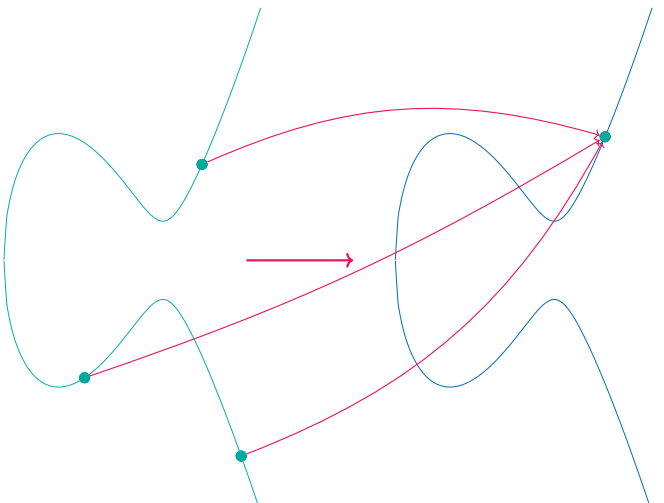
Supersingular Isogeny Diffie–Hellman

- SIDH °2011 (Jao & De Feo)
- Previous security:
  - generic attacks with complexity $\mathcal{O}(\sqrt[4]{p})$ classical and $\mathcal{O}(\sqrt[6]{p})$ quantum (claw finding);
  - attack on unbalanced parameters (de Quehen, Kutas, Leonardi, Martindale, Panny, Petit, Stange);
  - chosen ciphertext attack against static key SIDH (Galbraith, Petit, Shani, Ti).
- SIKE (Supersingular Isogeny Key Encapsulation) allows long term public keys.
- July 5th 2022: SIKE advances to Round 4 in NIST's post-quantum standardization process.
- This work: attack in (heuristic) polynomial time or subexponential time.

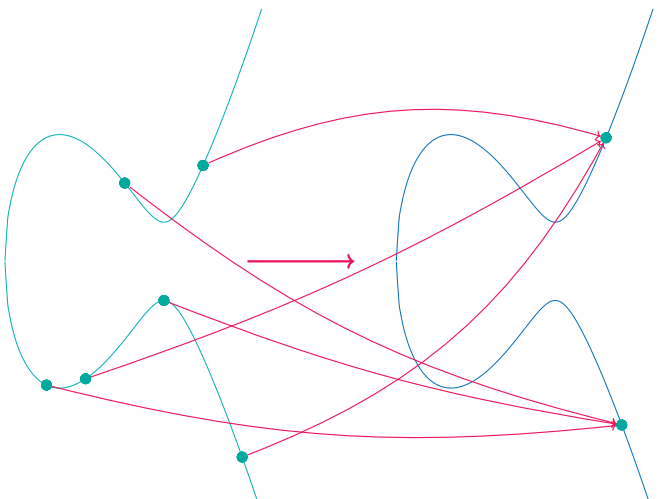
Isogenies



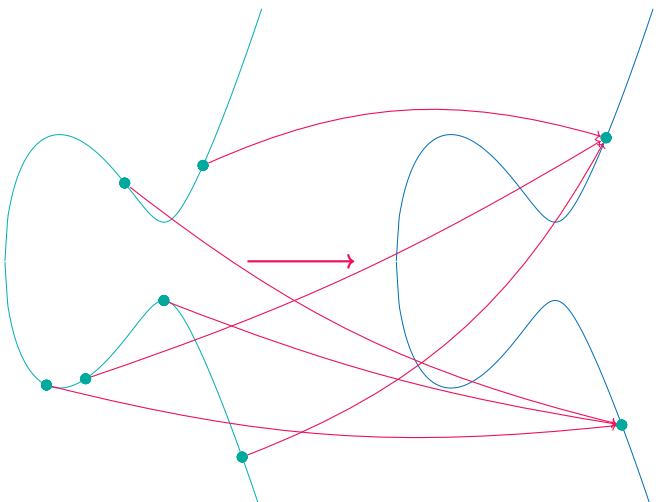
Isogenies



Isogenies

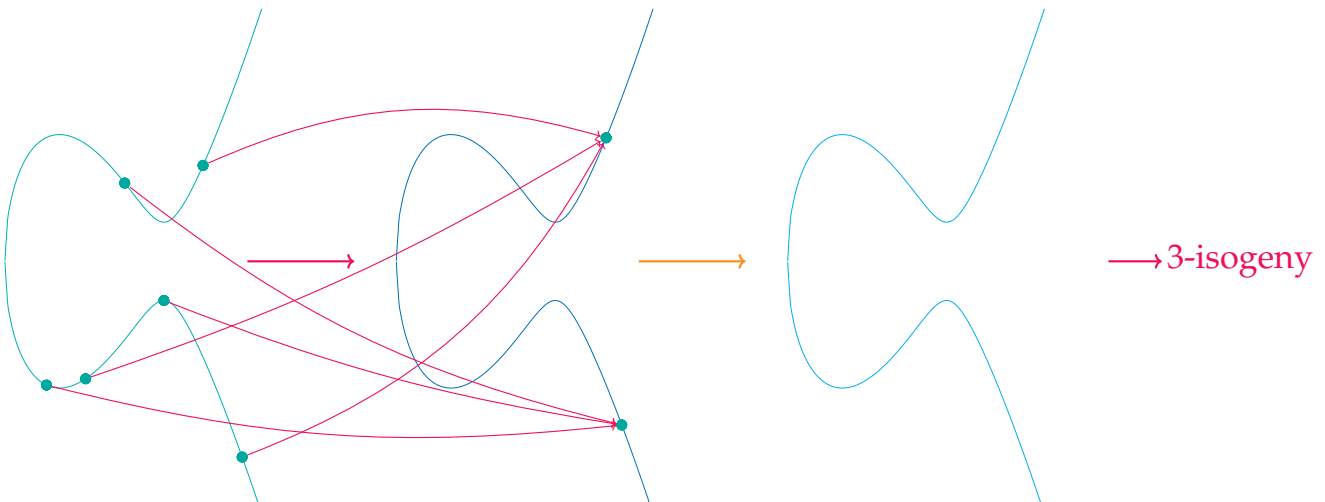


Isogenies

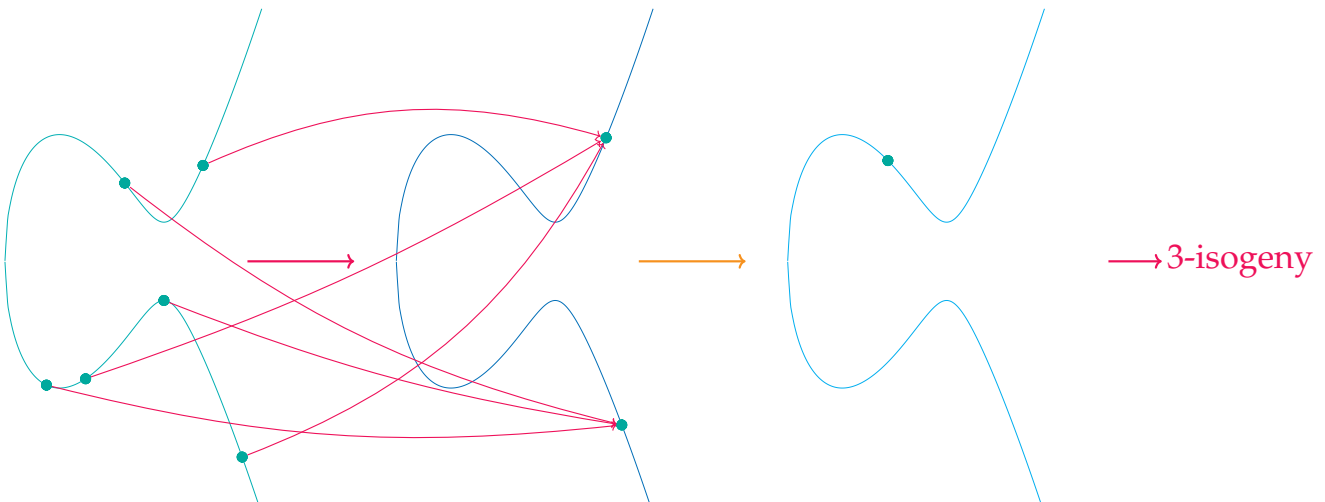


$\longrightarrow$ 3-isogeny

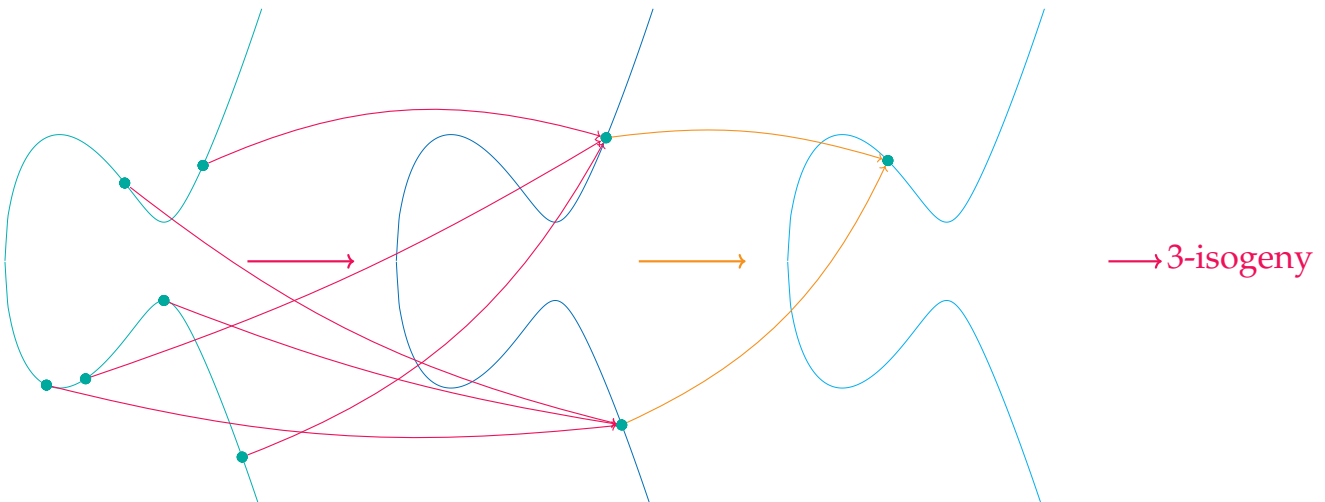
Isogenies



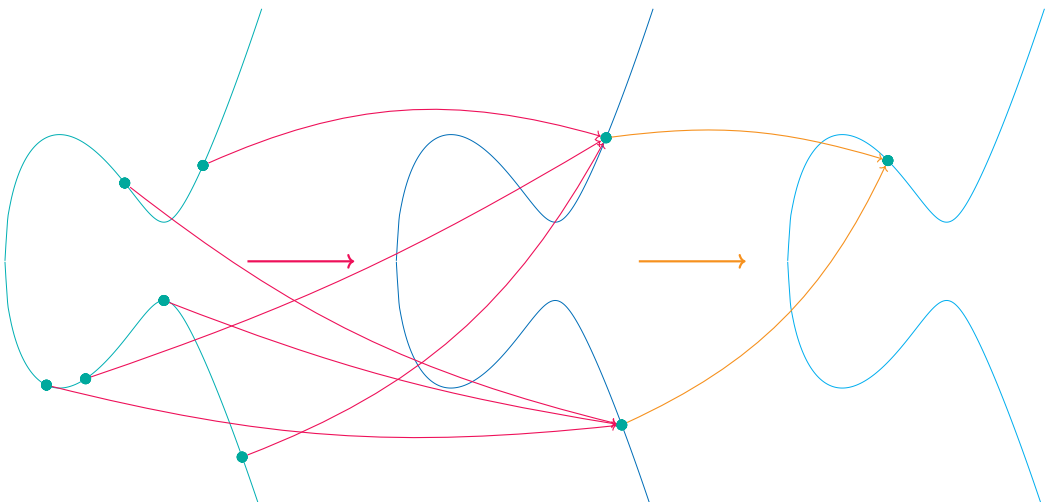
Isogenies



Isogenies



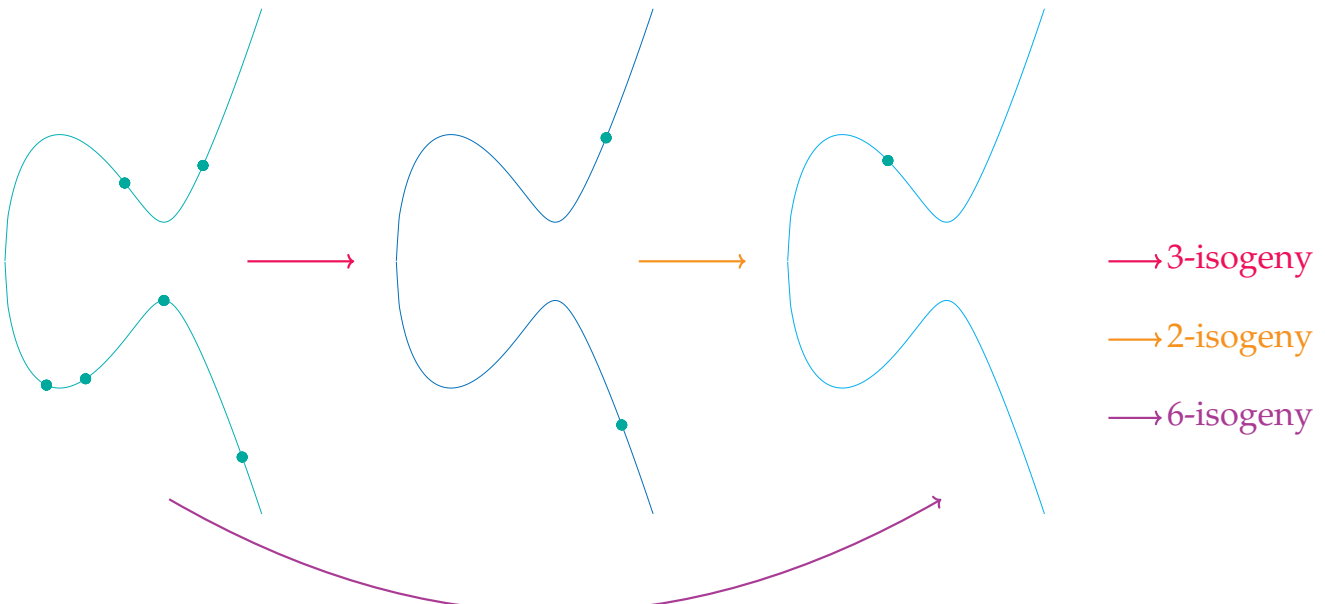
Isogenies



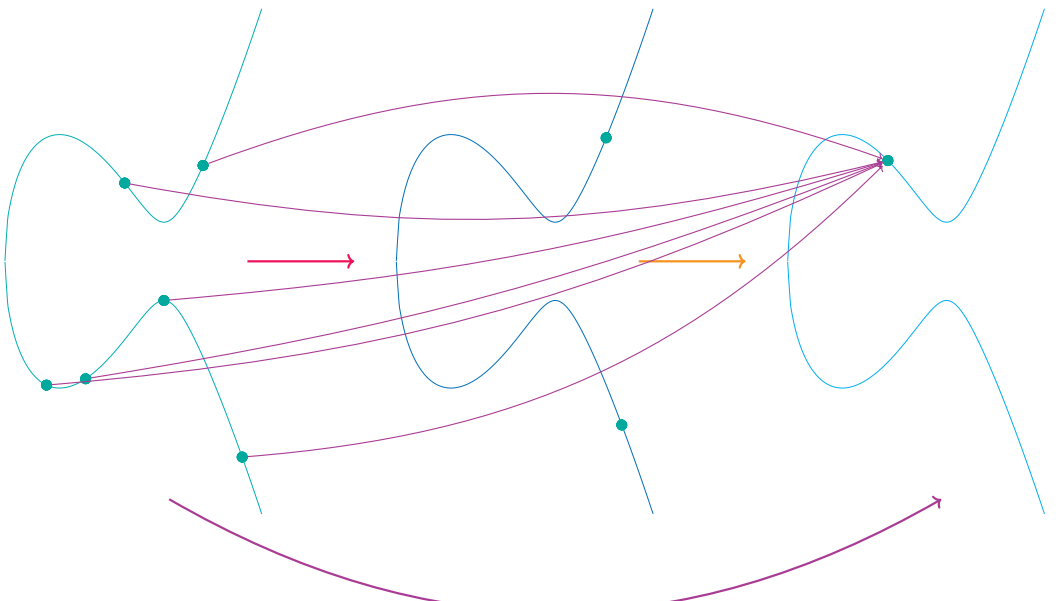
$\longrightarrow$ 3-isogeny

$\longrightarrow$ 2-isogeny

Isogenies



Isogenies

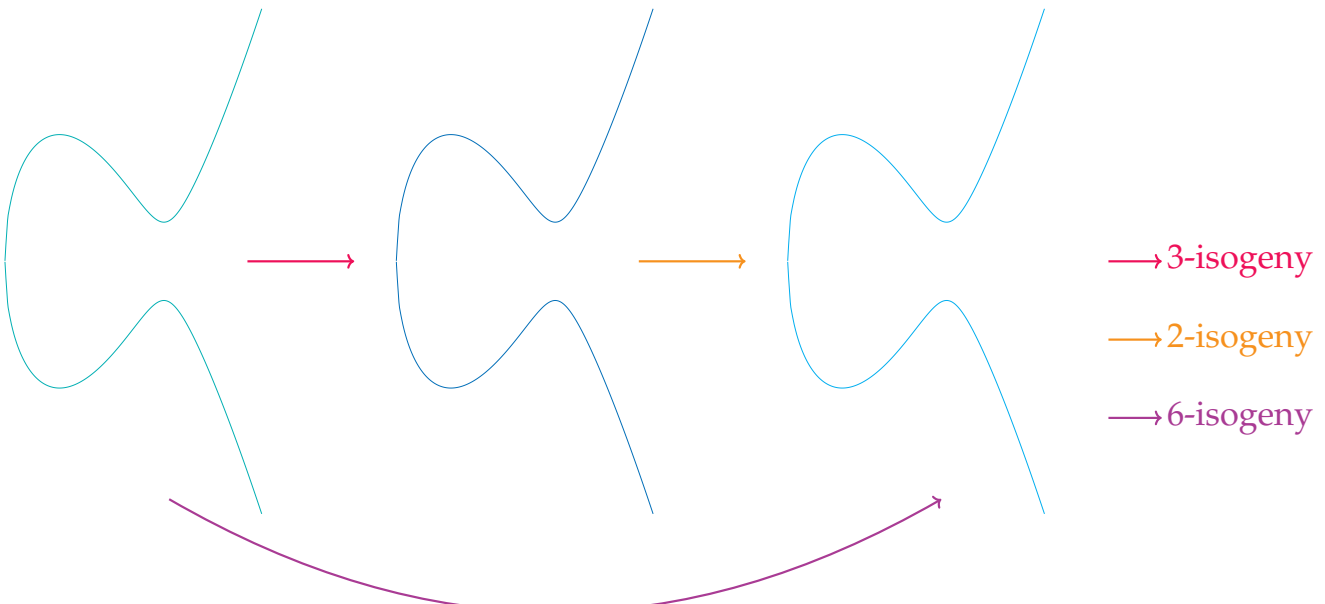


$\longrightarrow$ 3-isogeny

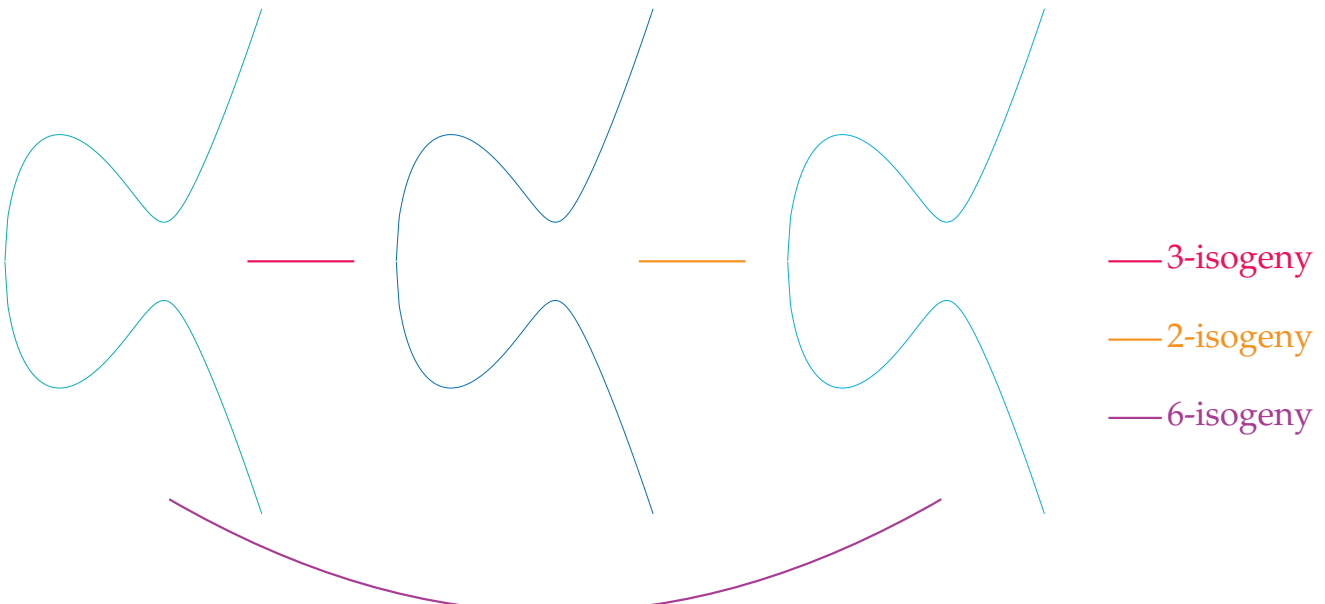
$\longrightarrow$ 2-isogeny

$\longrightarrow$ 6-isogeny

Isogenies

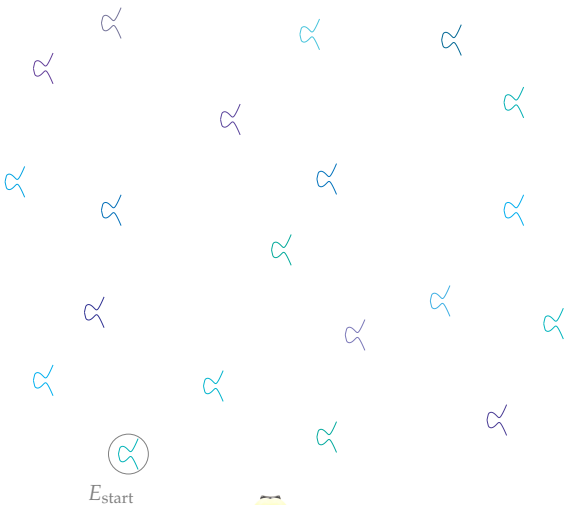


Isogenies

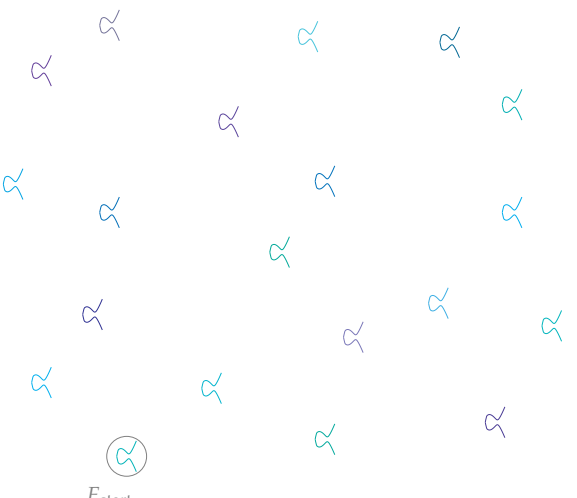


SIDH KEY EXCHANGE

SIDH KEY EXCHANGE

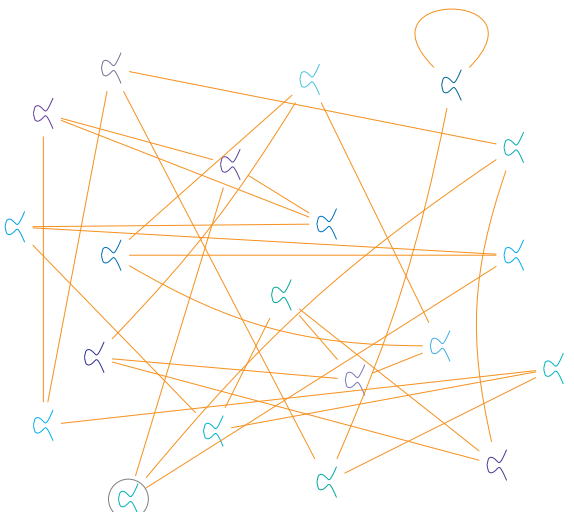


E_{start}



E_{start}

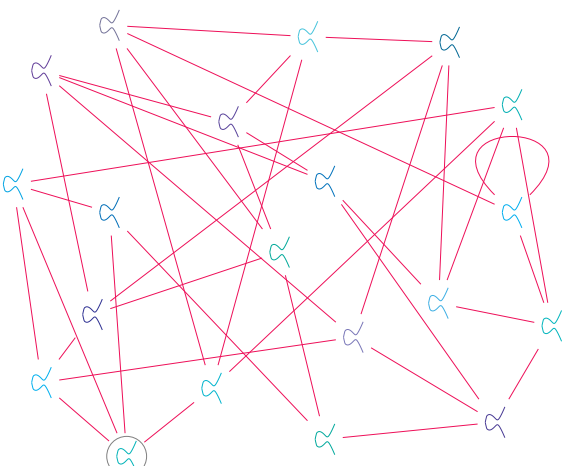
SIDH KEY EXCHANGE



E_{start}

— 2-isogeny

ALICE

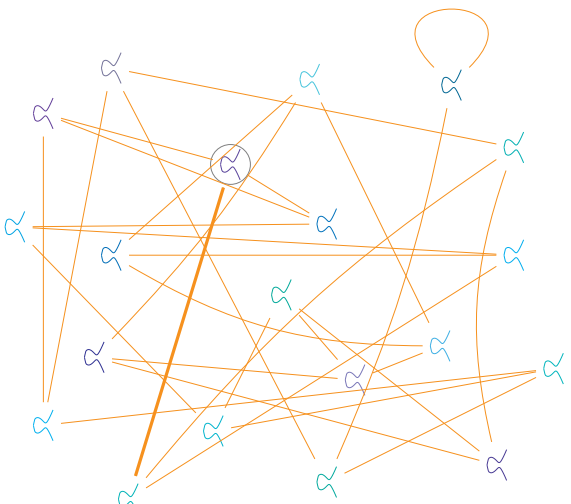


E_{start}

BOB

— 3-isogeny

SIDH KEY EXCHANGE

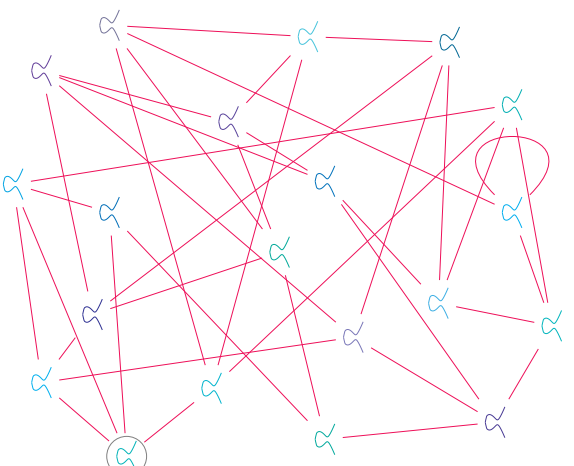


E_{start}

ALICE

2-isogeny

secret path

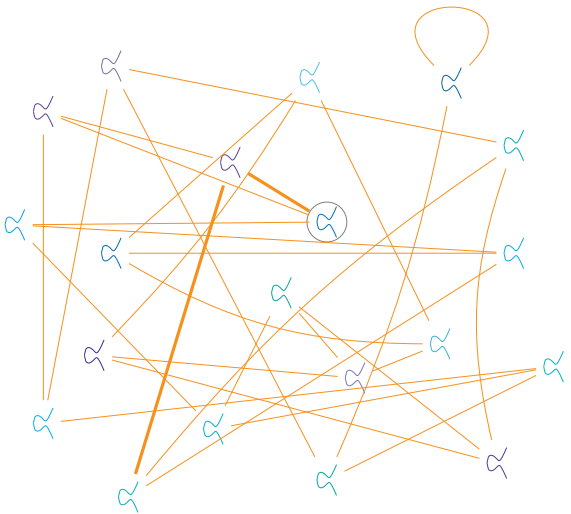


E_{start}

BOB

3-isogeny

SIDH KEY EXCHANGE

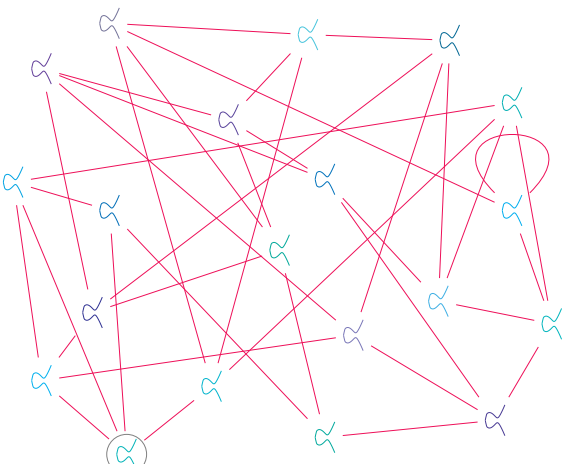


E_{start}

ALICE

2-isogeny

secret path

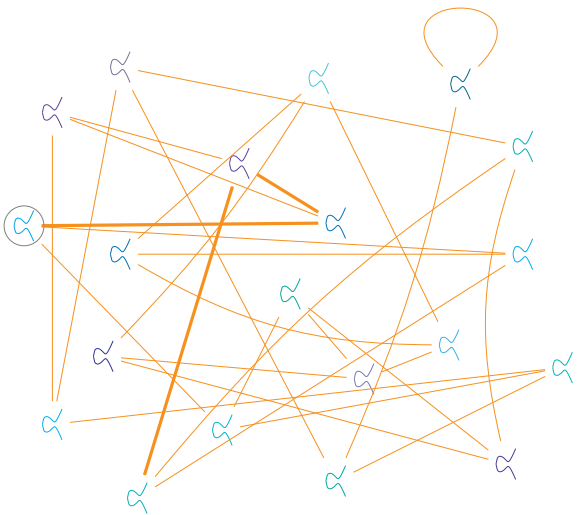


E_{start}

BOB

3-isogeny

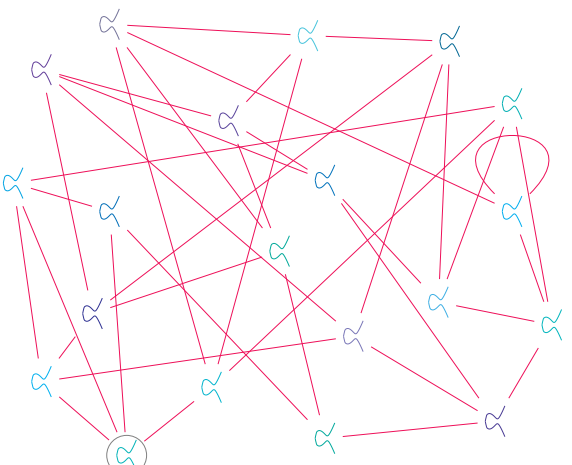
SIDH KEY EXCHANGE



E_{start}

2-isogeny

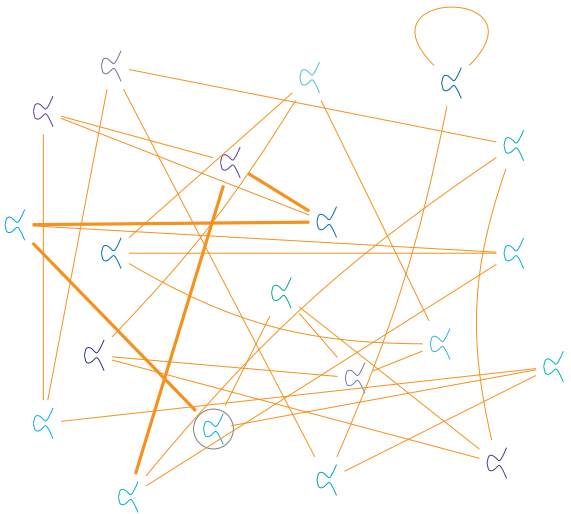
secret path



E_{start}

3-isogeny

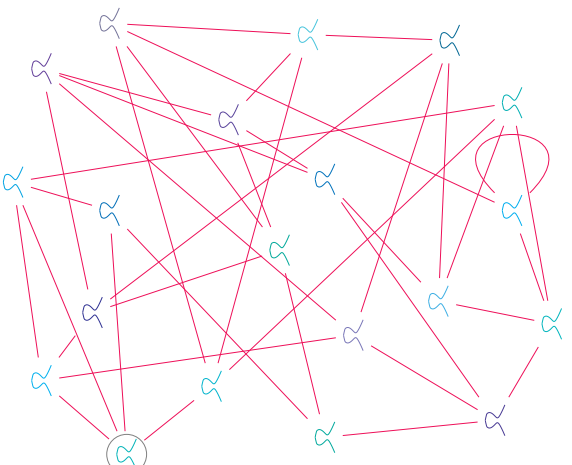
SIDH KEY EXCHANGE



E_{start}

2-isogeny

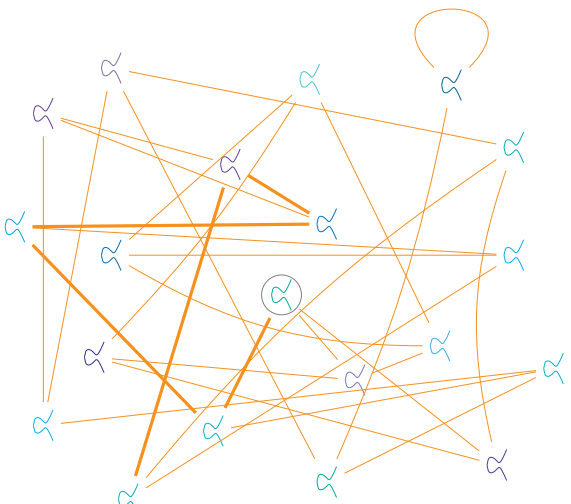
secret path



E_{start}

3-isogeny

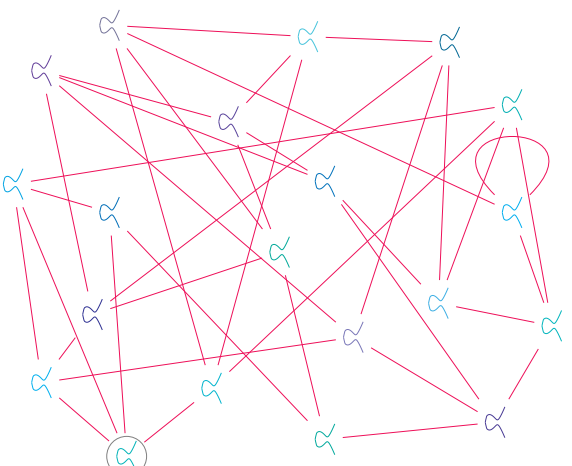
SIDH KEY EXCHANGE



E_{start}

— 2-isogeny

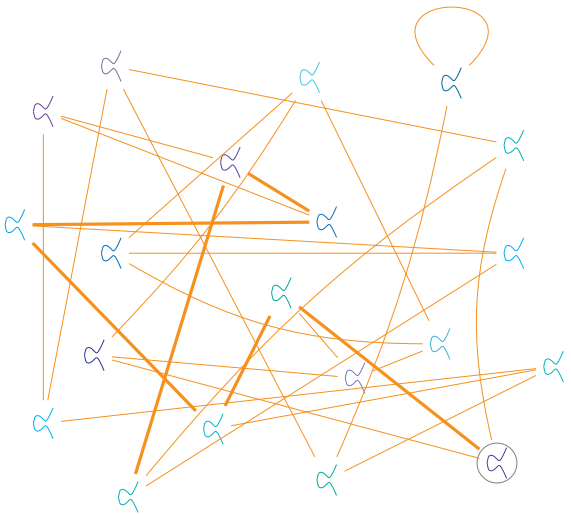
— secret path



E_{start}

— 3-isogeny

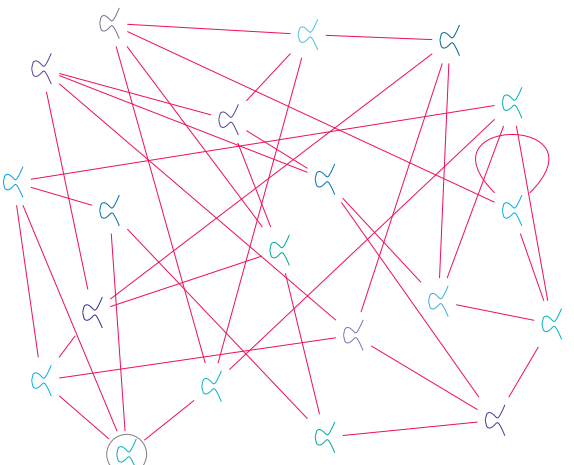
SIDH KEY EXCHANGE



E_{start}

2-isogeny

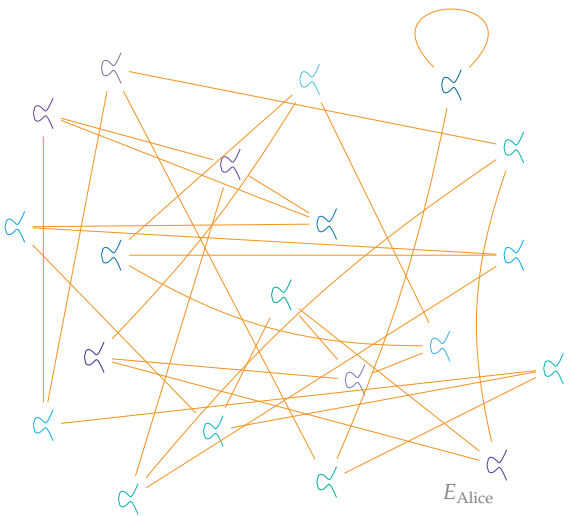
secret path

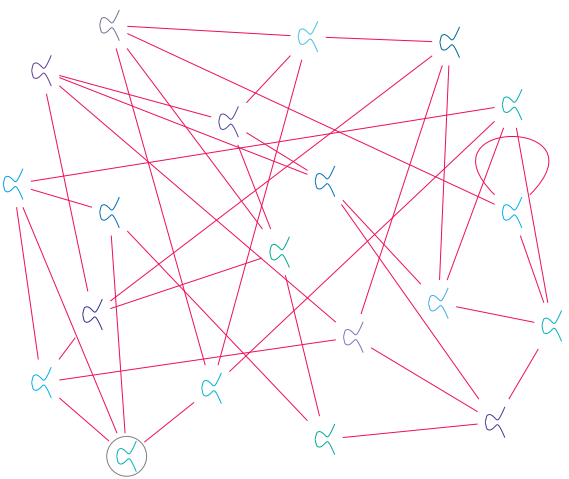


E_{start}

3-isogeny

SIDH KEY EXCHANGE

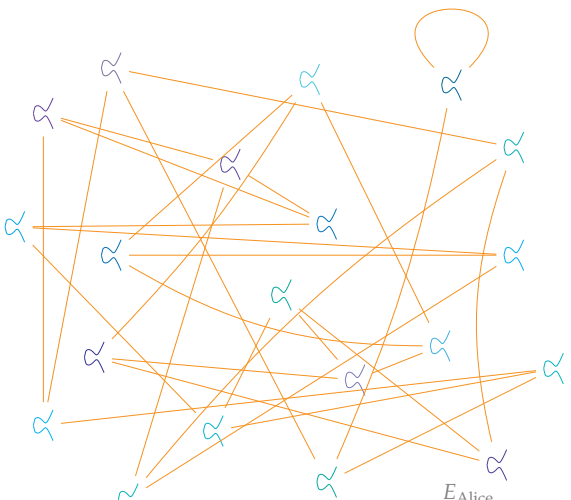




— 2-isogeny
— secret path

— 3-isogeny

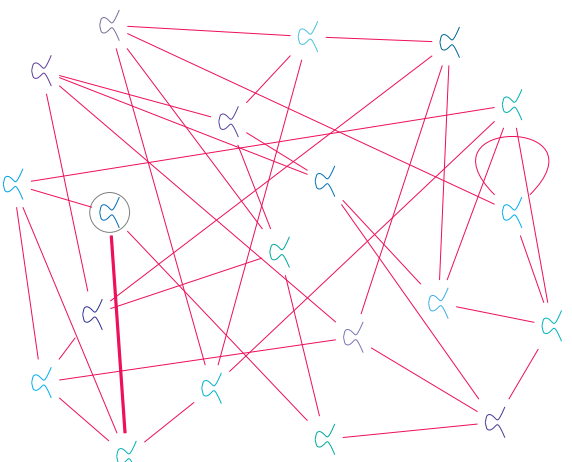
SIDH KEY EXCHANGE



E_{start}

2-isogeny

secret path

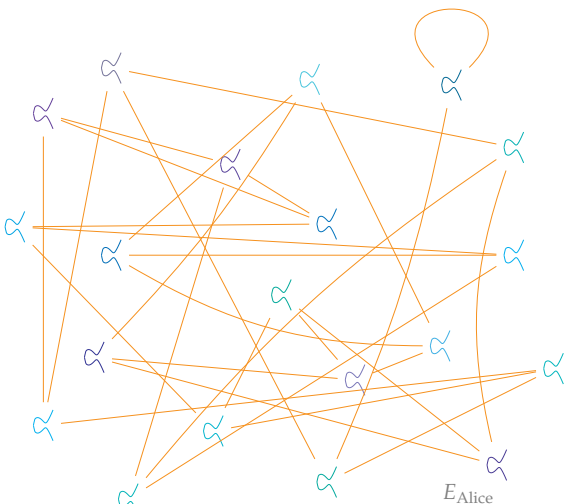


E_{start}

3-isogeny

secret path

SIDH KEY EXCHANGE

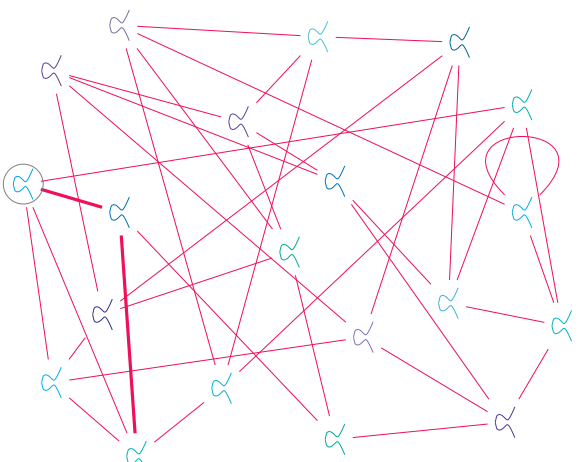


E_{start}

ALICE

2-isogeny

secret path



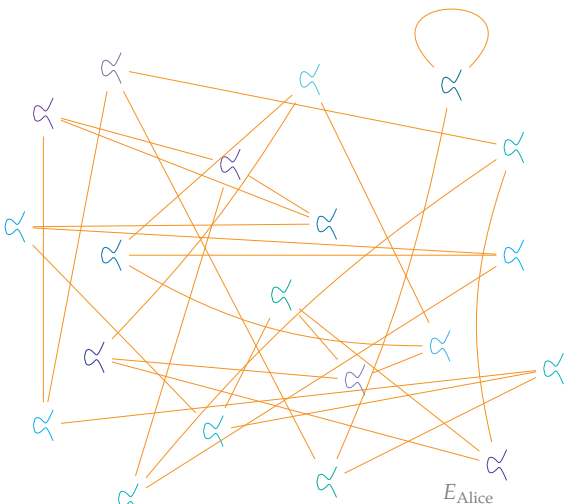
E_{start}

BOB

3-isogeny

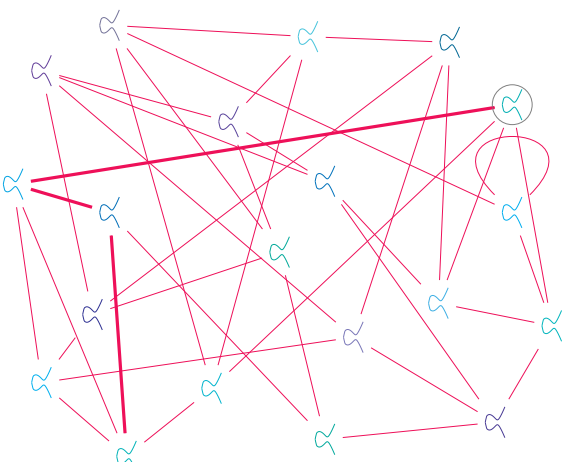
secret path

SIDH KEY EXCHANGE



E_{start}

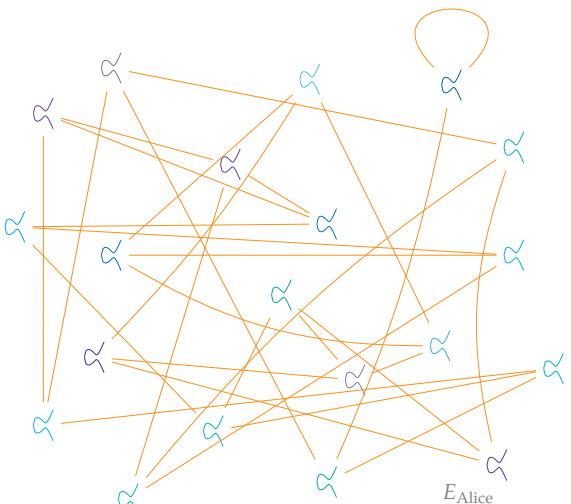
2-isogeny
secret path



E_{start}

3-isogeny
secret path

SIDH KEY EXCHANGE

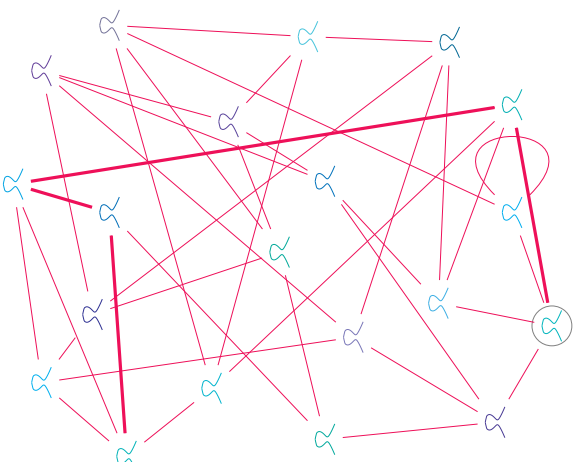


E_{start}

ALICE

2-isogeny

secret path



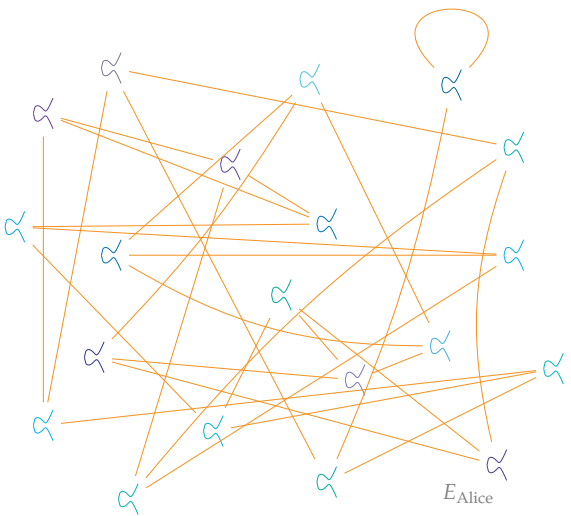
E_{start}

BOB

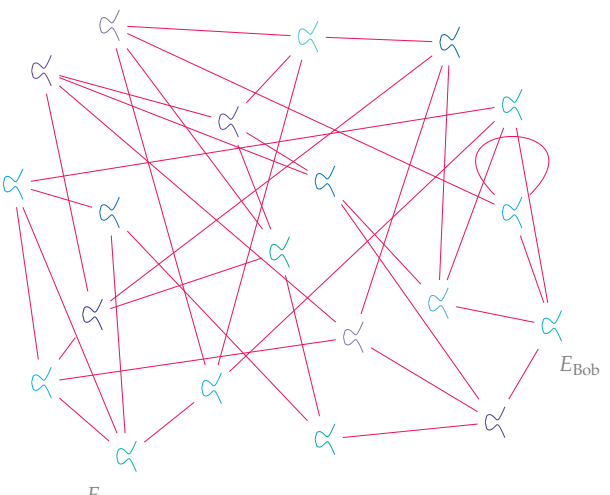
3-isogeny

secret path

SIDH KEY EXCHANGE

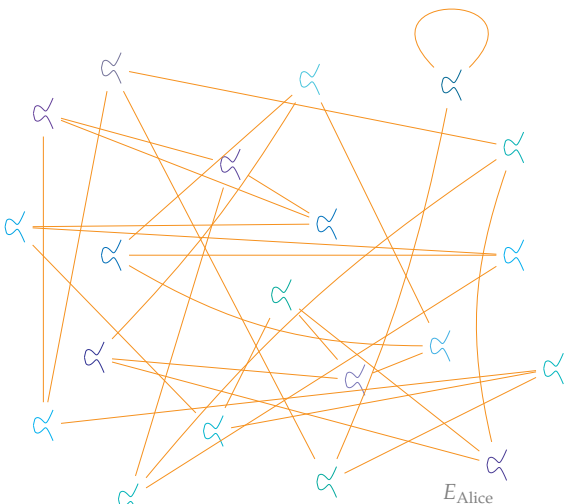


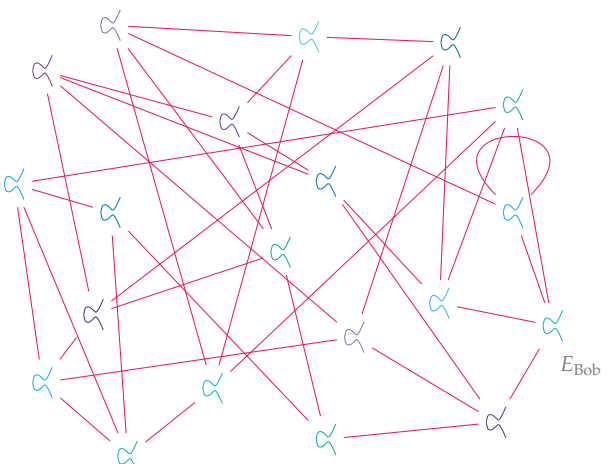
2-isogeny
secret path



3-isogeny
secret path

SIDH KEY EXCHANGE





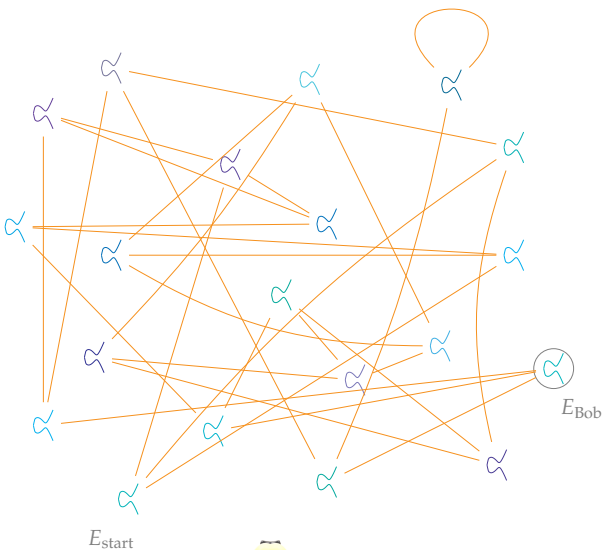
2-isogeny
secret path

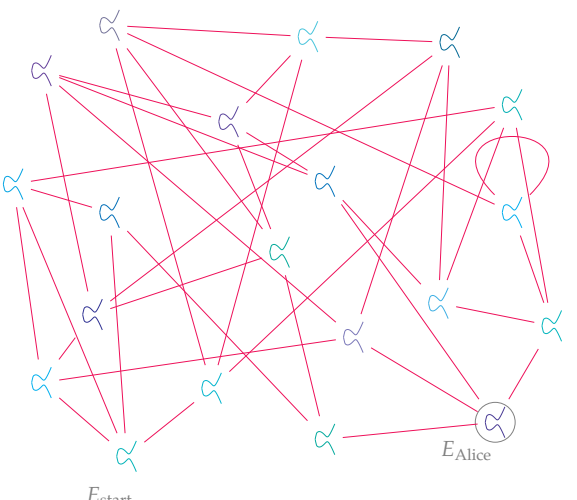
E_{Alice}

E_{Bob}

3-isogeny
secret path

SIDH KEY EXCHANGE

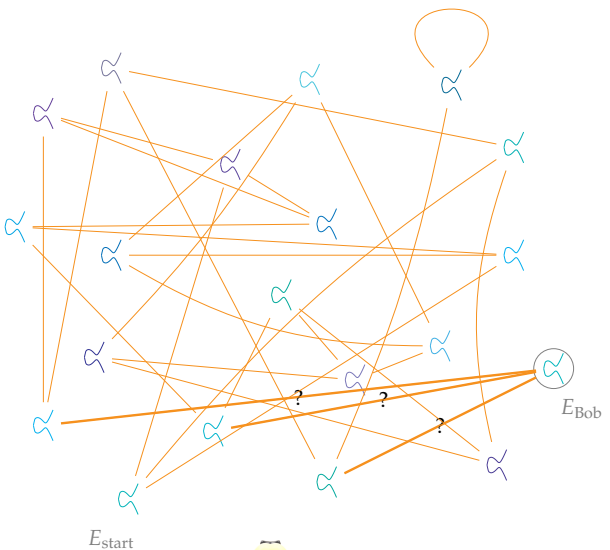


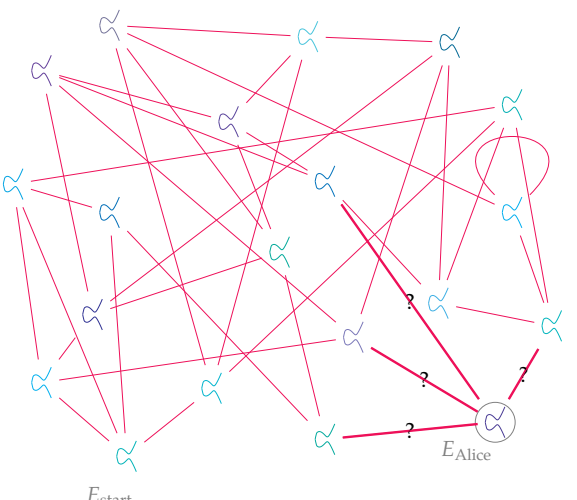


2-isogeny
secret path

3-isogeny
secret path

SIDH KEY EXCHANGE

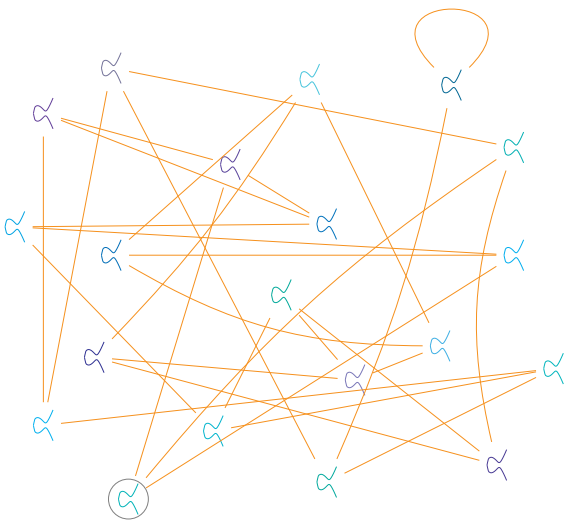




2-isogeny
secret path

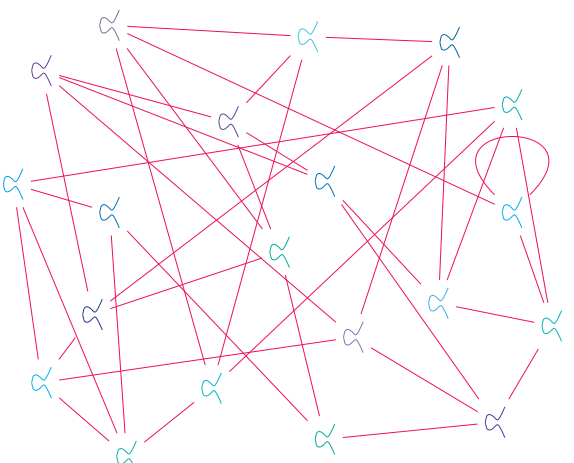
3-isogeny
secret path

SIDH KEY EXCHANGE



E_{start}

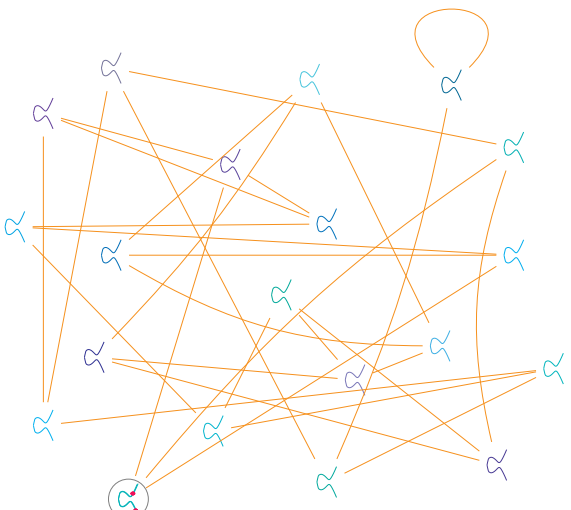
2-isogeny
secret path



E_{start}

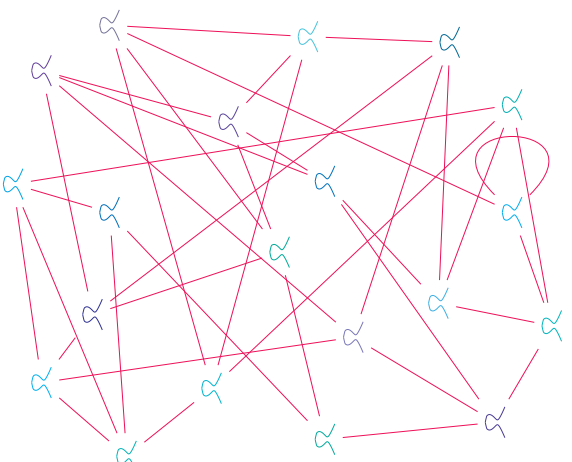
3-isogeny
secret path

SIDH KEY EXCHANGE



E_{start}

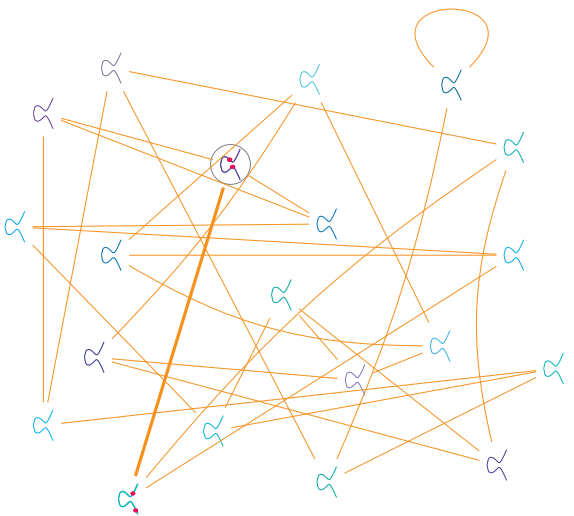
2-isogeny
secret path



E_{start}

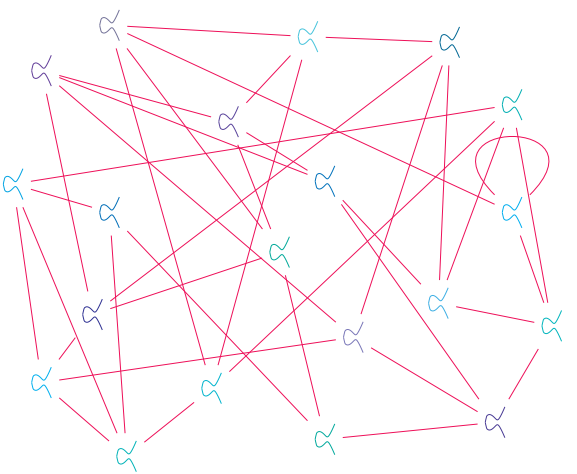
3-isogeny
secret path

SIDH KEY EXCHANGE



E_{start}

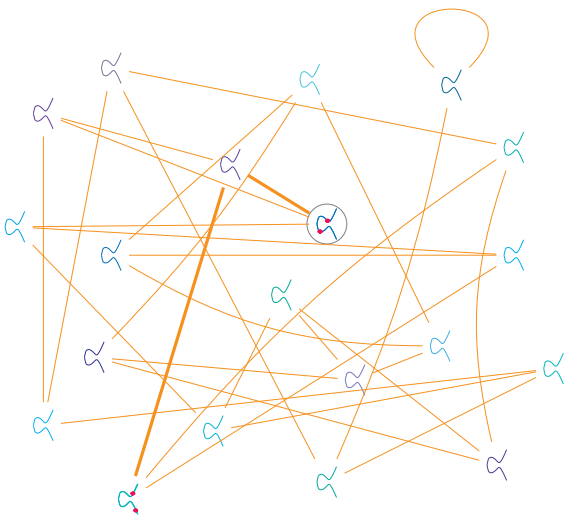
2-isogeny
secret path



E_{start}

3-isogeny
secret path

SIDH KEY EXCHANGE

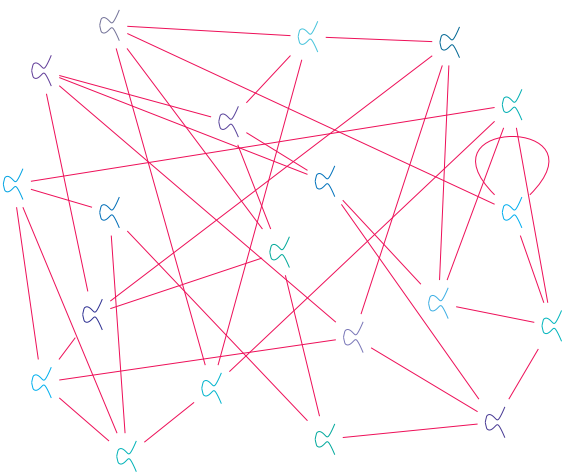


E_{start}

ALICE

2-isogeny

secret path



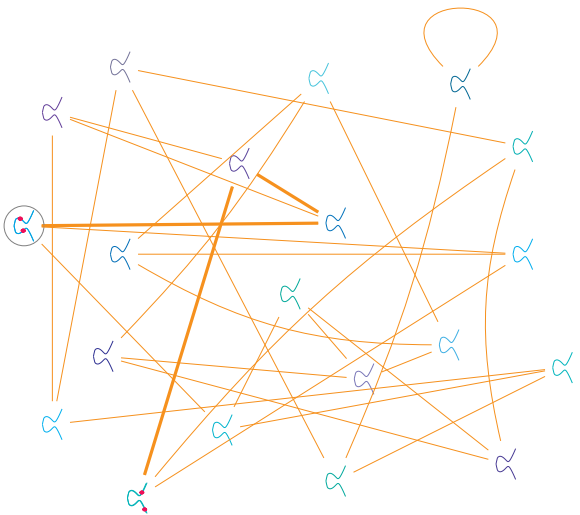
E_{start}

BOB

3-isogeny

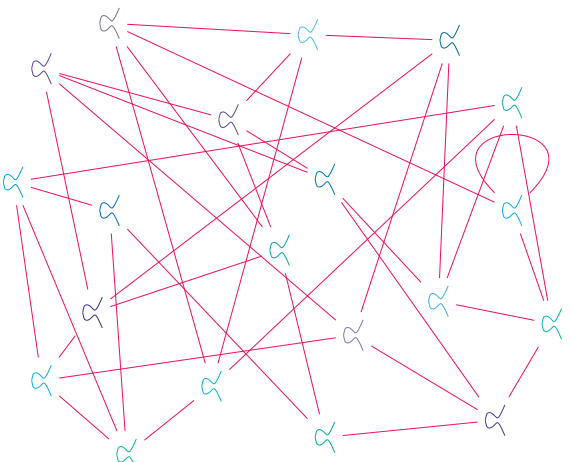
secret path

SIDH KEY EXCHANGE



E_{start}

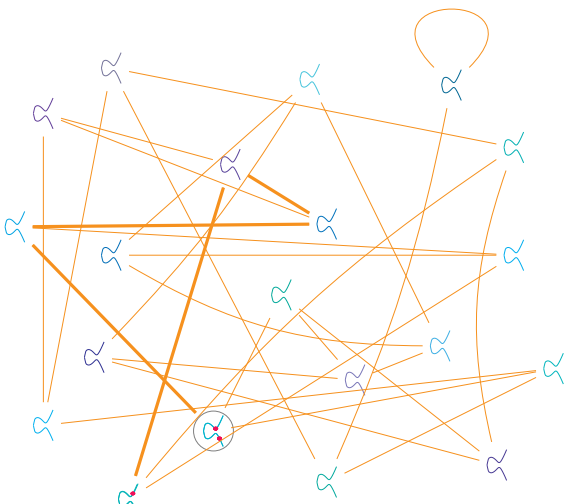
2-isogeny
secret path



E_{start}

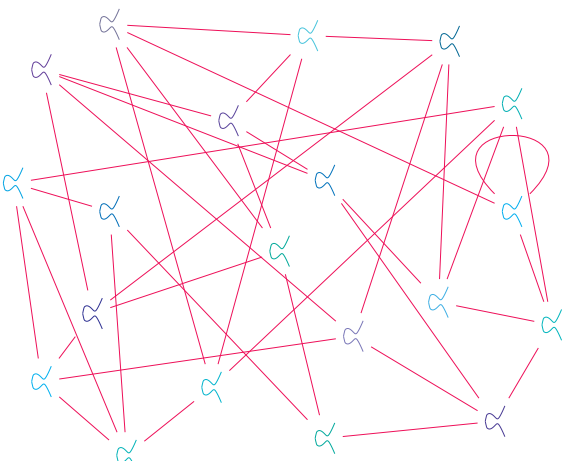
3-isogeny
secret path

SIDH KEY EXCHANGE



E_{start}

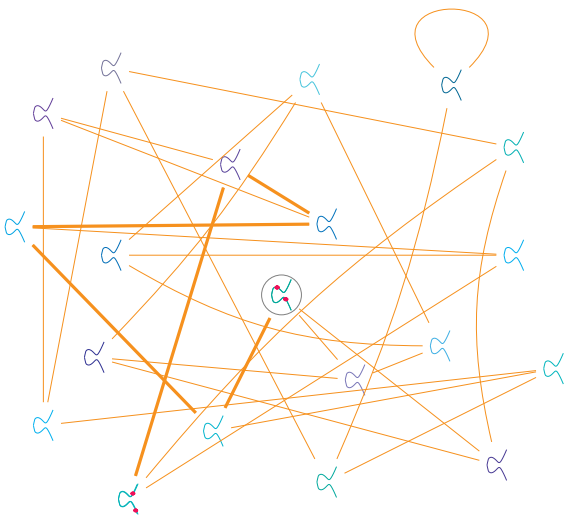
2-isogeny
secret path



E_{start}

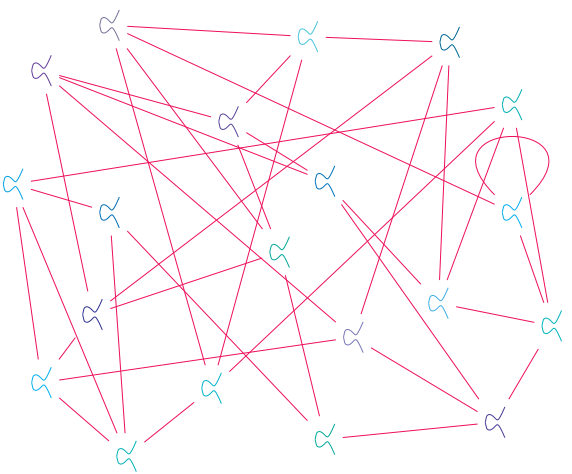
3-isogeny
secret path

SIDH KEY EXCHANGE



E_{start}

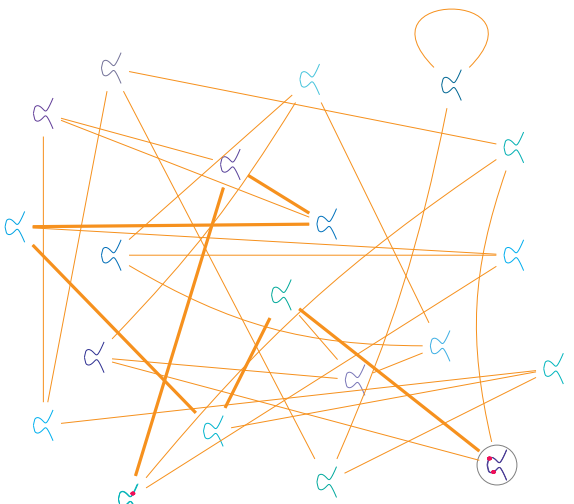
2-isogeny
secret path



E_{start}

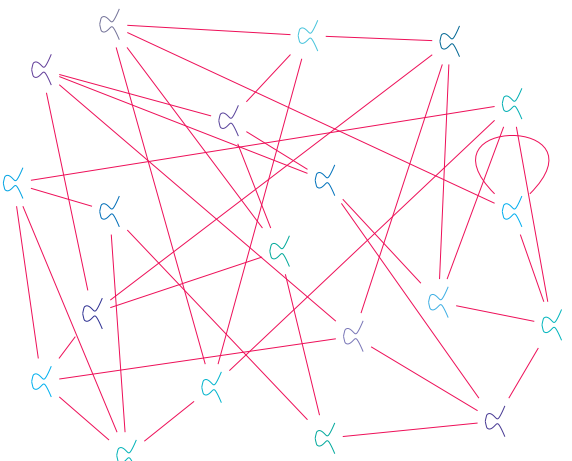
3-isogeny
secret path

SIDH KEY EXCHANGE



E_{start}

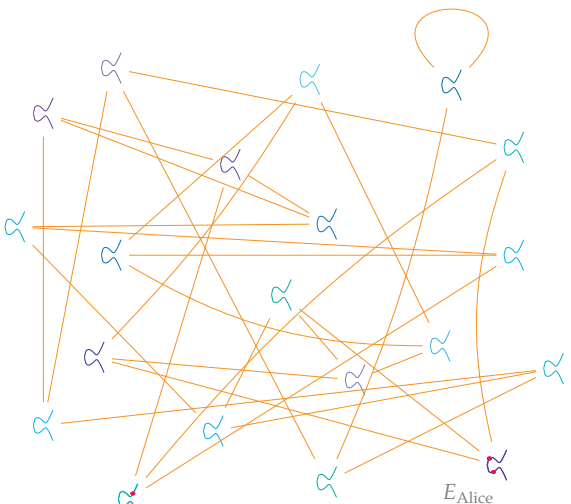
2-isogeny
secret path



E_{start}

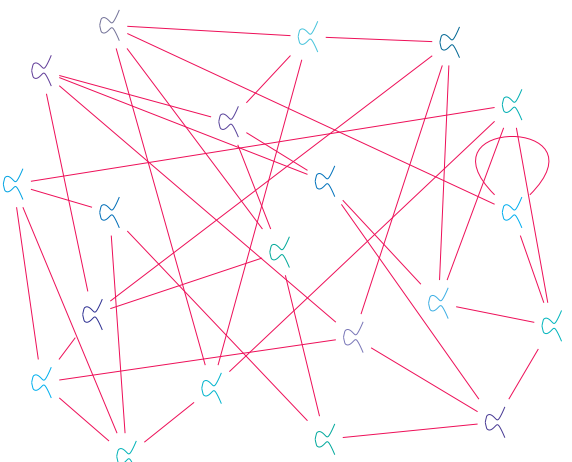
3-isogeny
secret path

SIDH KEY EXCHANGE



E_{start}

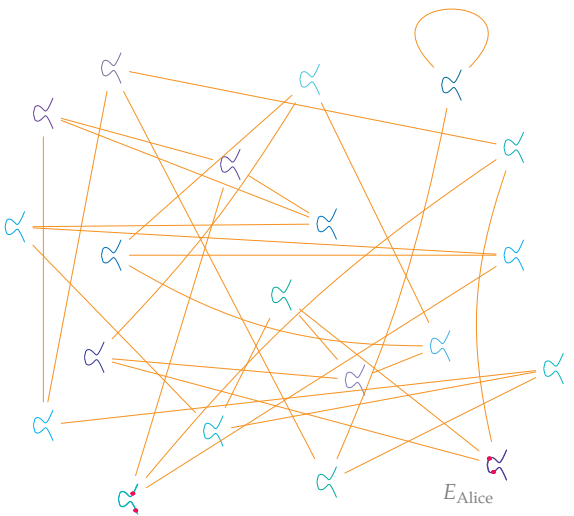
2-isogeny
secret path



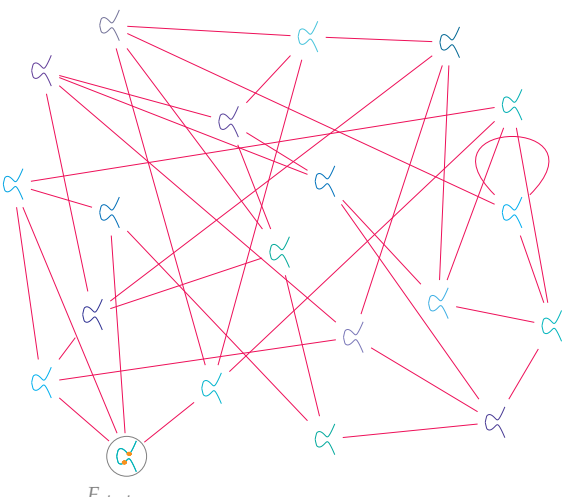
E_{start}

3-isogeny
secret path

SIDH KEY EXCHANGE

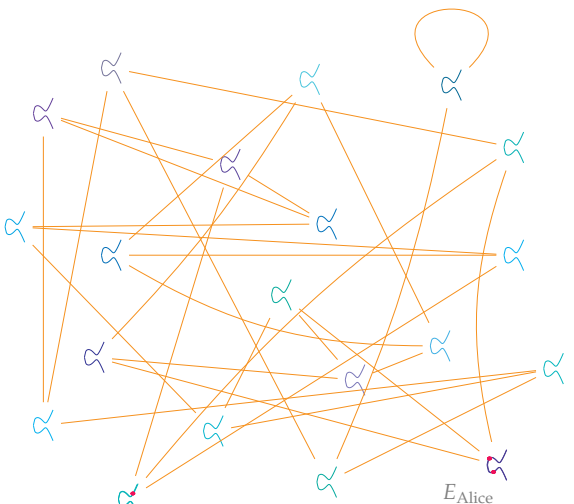


2-isogeny
secret path



3-isogeny
secret path

SIDH KEY EXCHANGE

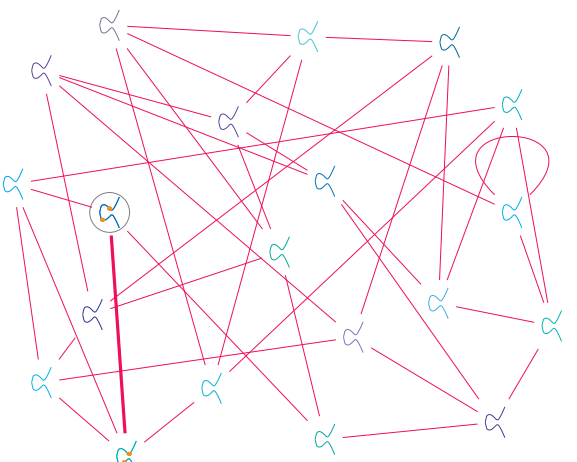


E_{start}

ALICE

2-isogeny

secret path



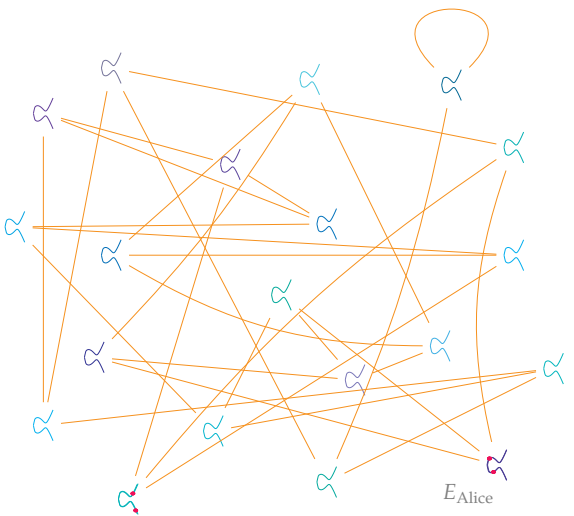
E_{start}

BOB

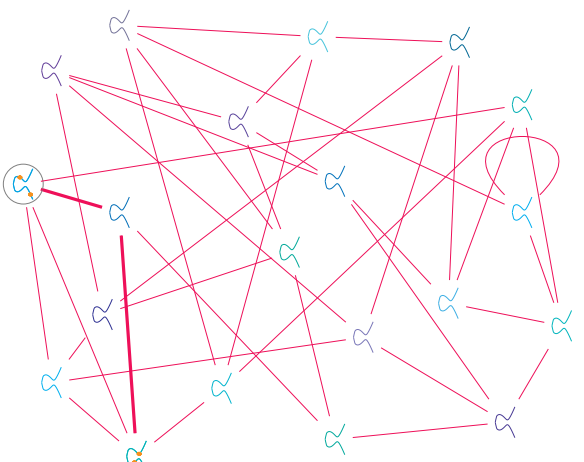
3-isogeny

secret path

SIDH KEY EXCHANGE

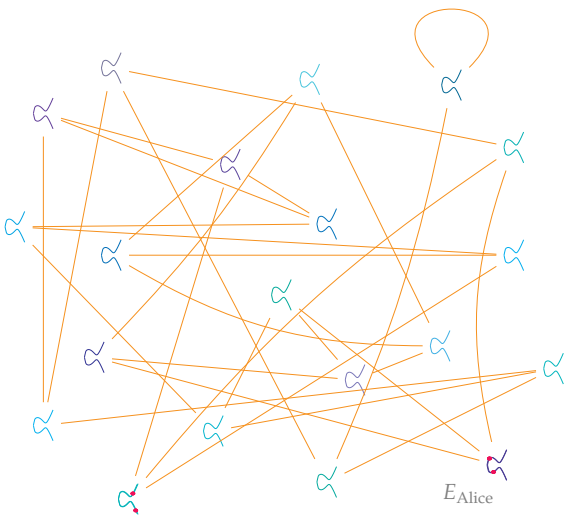


2-isogeny
secret path



3-isogeny
secret path

SIDH KEY EXCHANGE

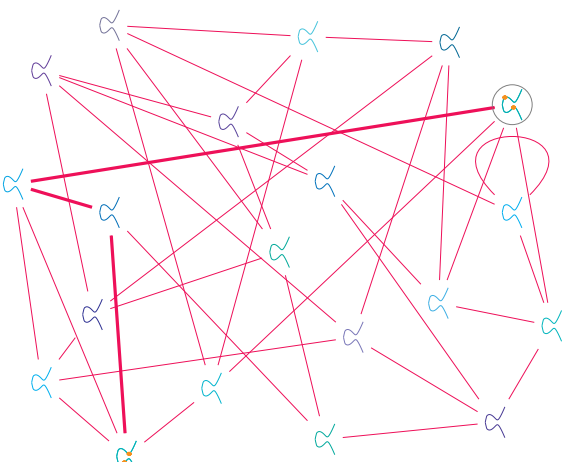


E_{start}

ALICE

2-isogeny

secret path



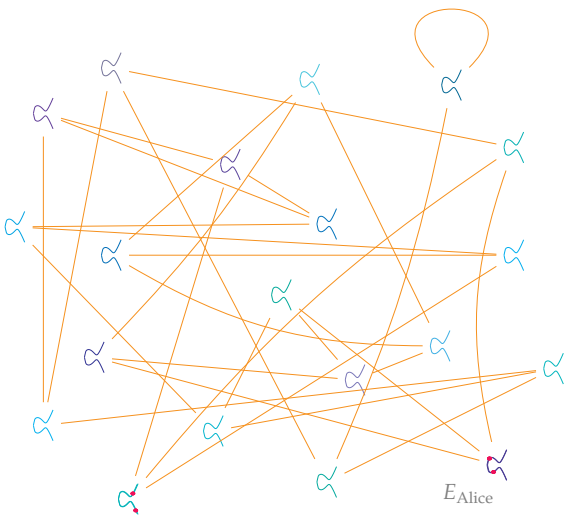
E_{start}

BOB

3-isogeny

secret path

SIDH KEY EXCHANGE

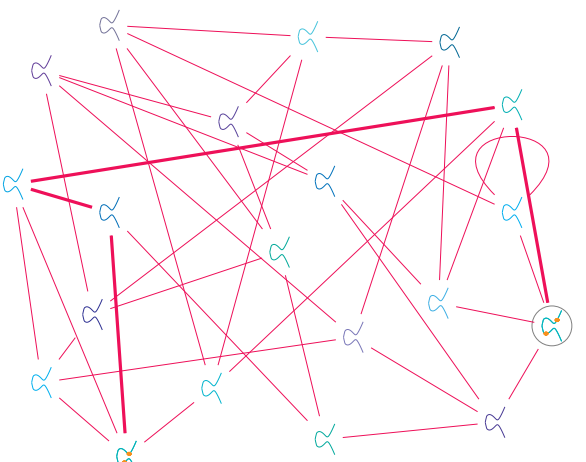


E_{start}

ALICE

2-isogeny

secret path



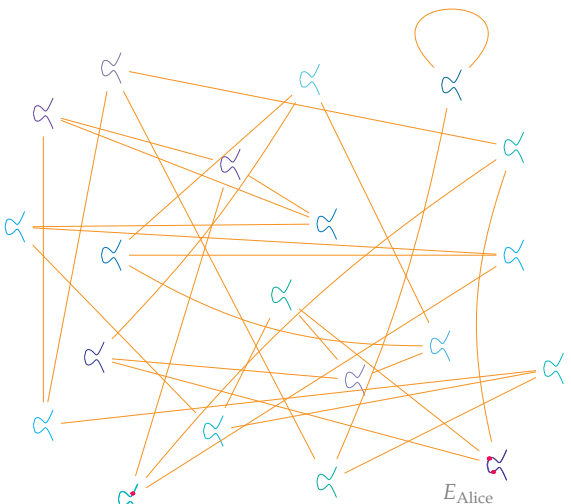
E_{start}

BOB

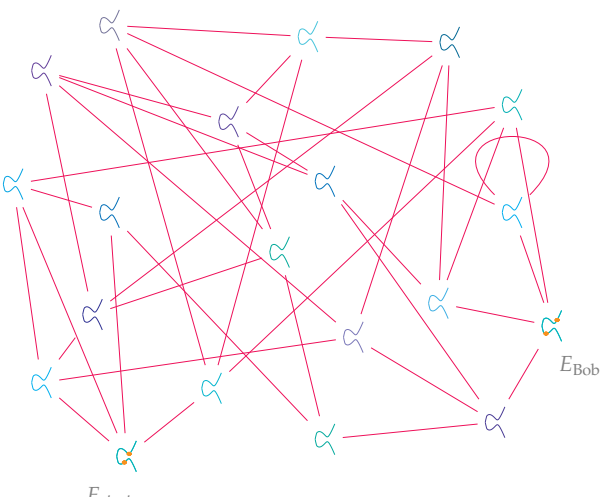
3-isogeny

secret path

SIDH KEY EXCHANGE

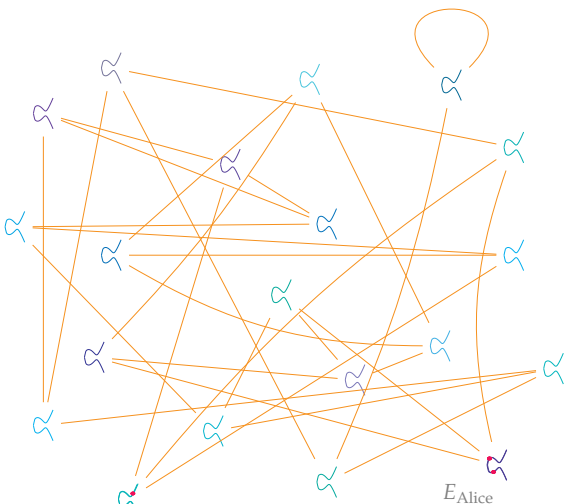


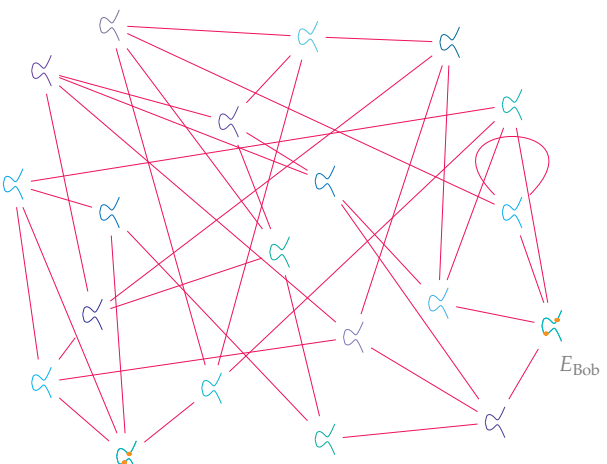
2-isogeny
secret path



3-isogeny
secret path

SIDH KEY EXCHANGE





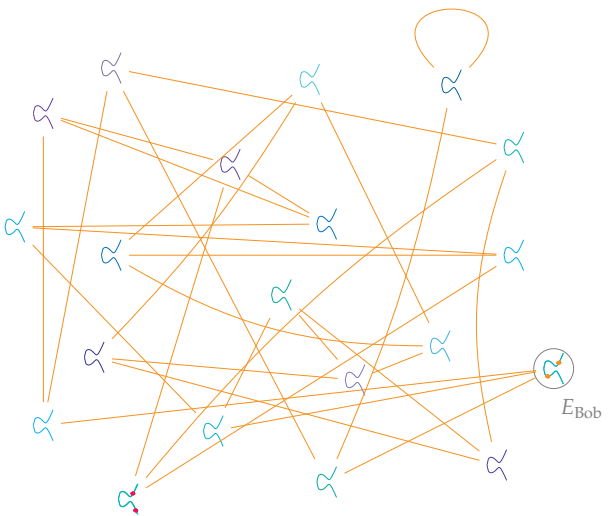
2-isogeny
secret path

E_{Alice}

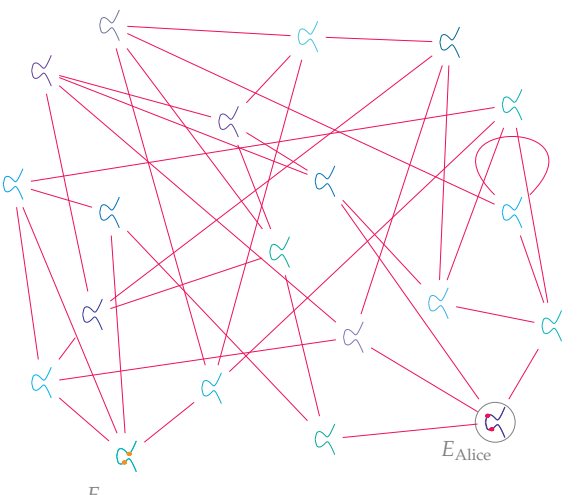
E_{Bob}

3-isogeny
secret path

SIDH KEY EXCHANGE

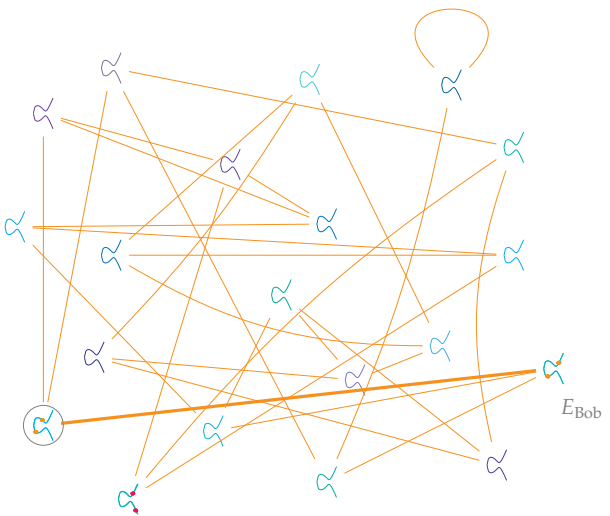


2-isogeny
secret path

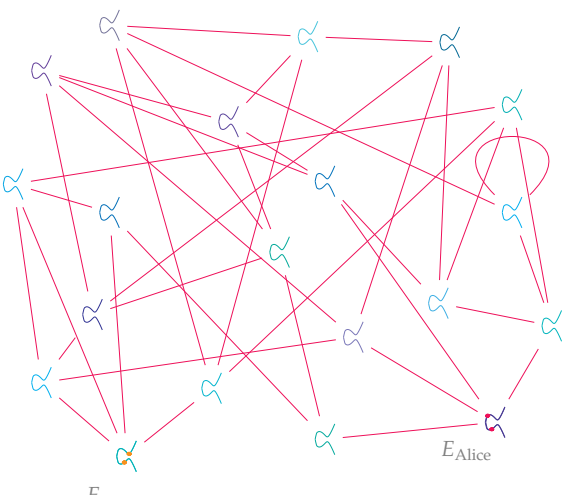


3-isogeny
secret path

SIDH KEY EXCHANGE

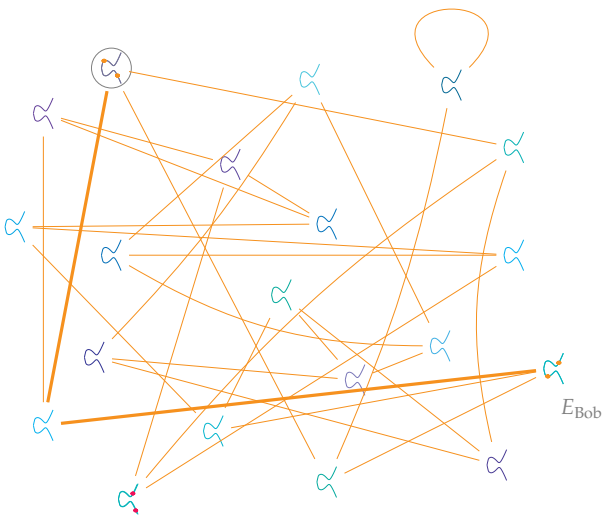


2-isogeny
secret path

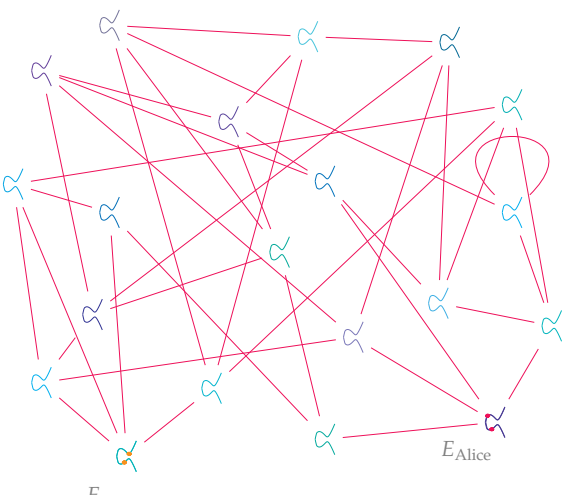


3-isogeny
secret path

SIDH KEY EXCHANGE

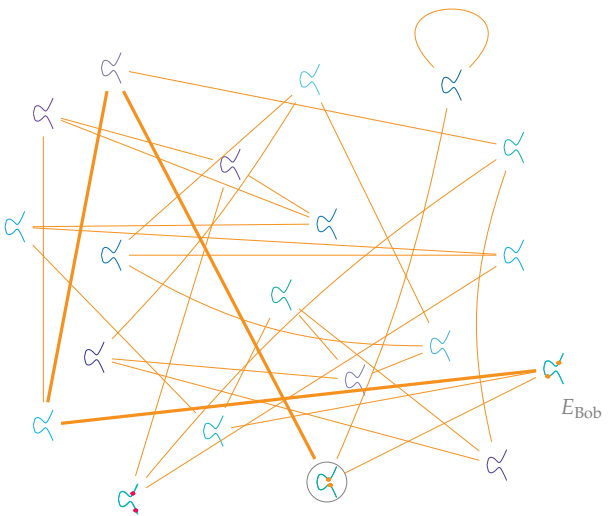


2-isogeny
secret path

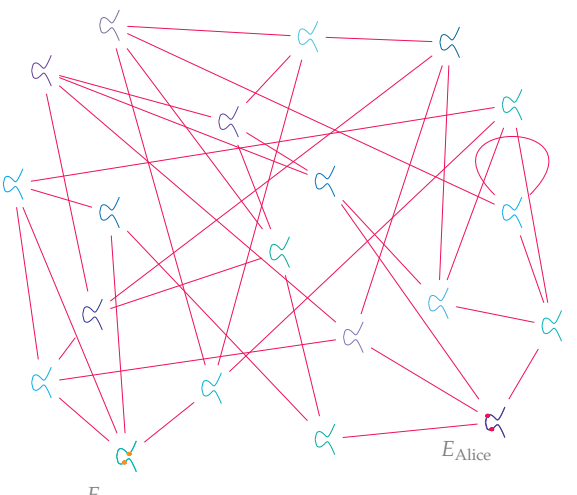


3-isogeny
secret path

SIDH KEY EXCHANGE

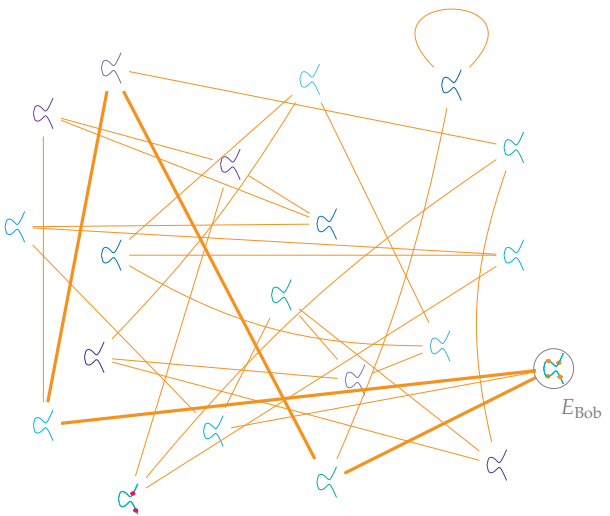


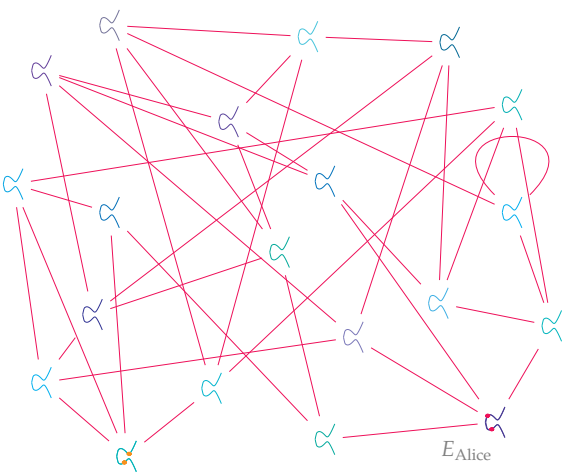
2-isogeny
secret path



3-isogeny
secret path

SIDH KEY EXCHANGE

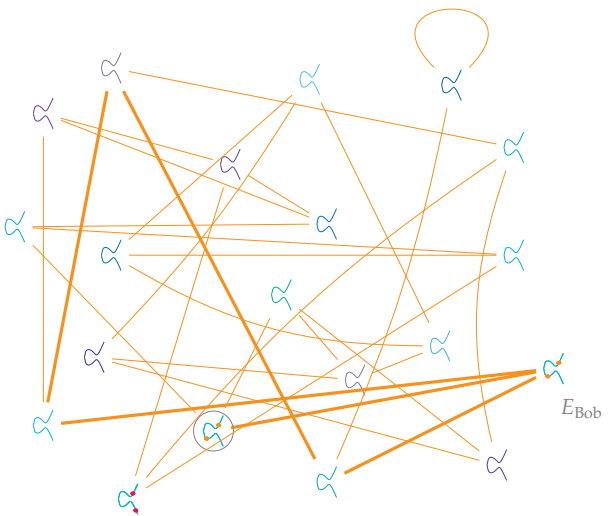


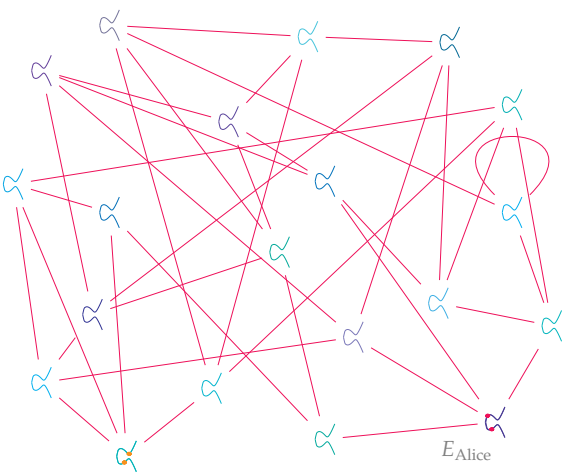


2-isogeny
secret path

3-isogeny
secret path

SIDH KEY EXCHANGE

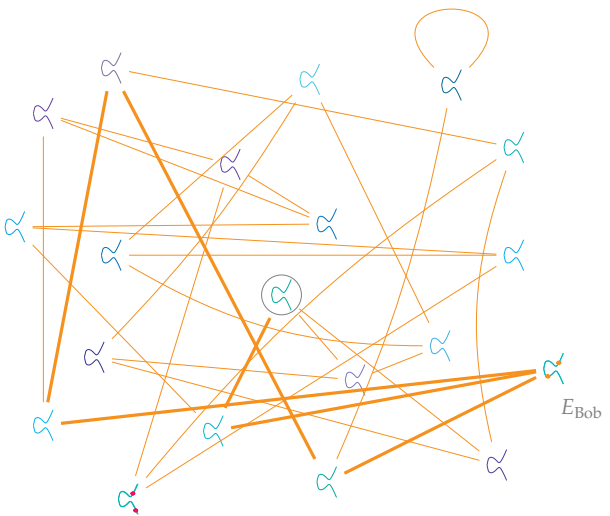


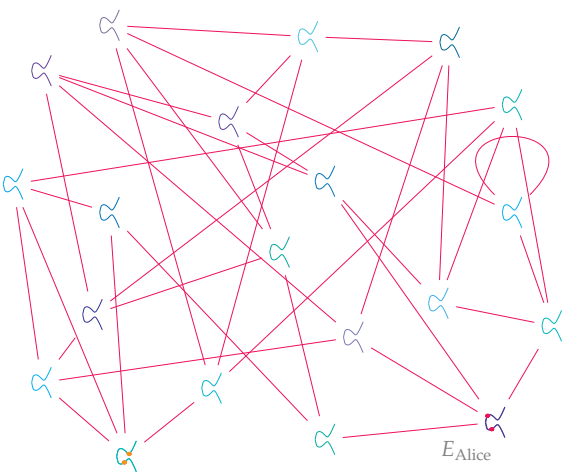


2-isogeny
secret path

3-isogeny
secret path

SIDH KEY EXCHANGE

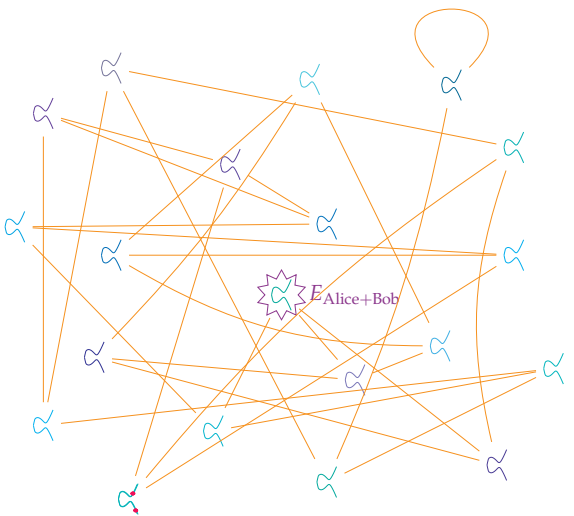




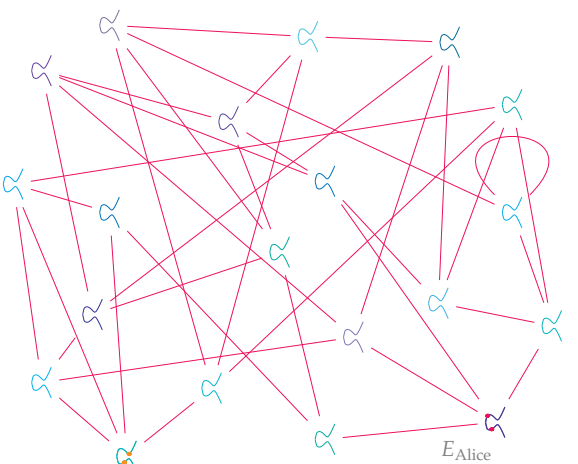
2-isogeny
secret path

3-isogeny
secret path

SIDH KEY EXCHANGE

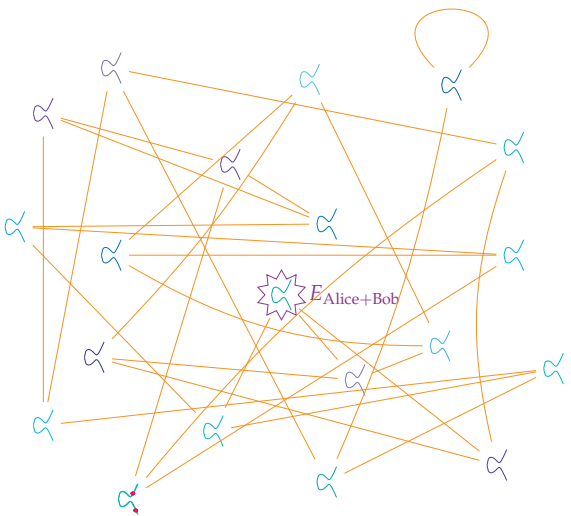


2-isogeny
secret path

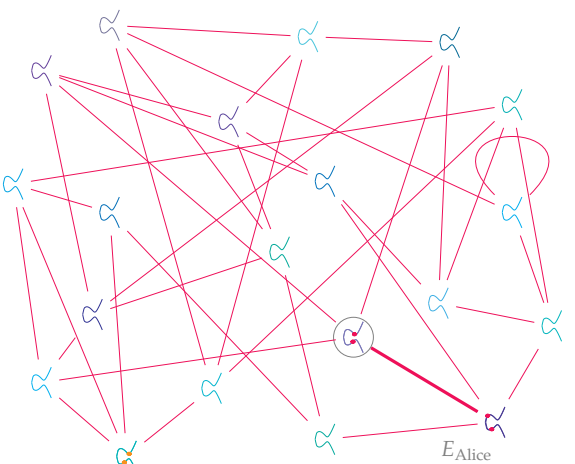


3-isogeny
secret path

SIDH KEY EXCHANGE

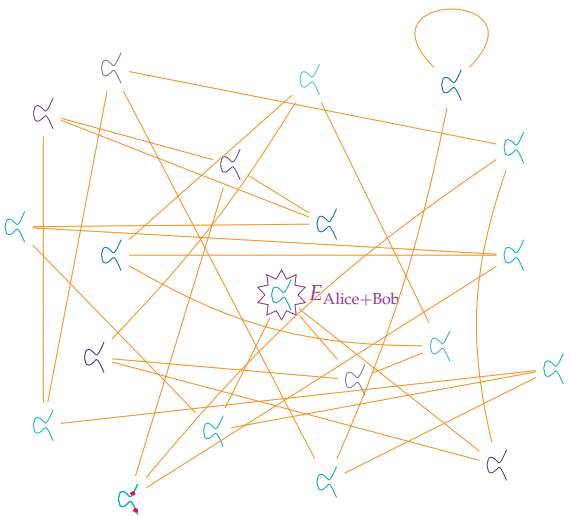


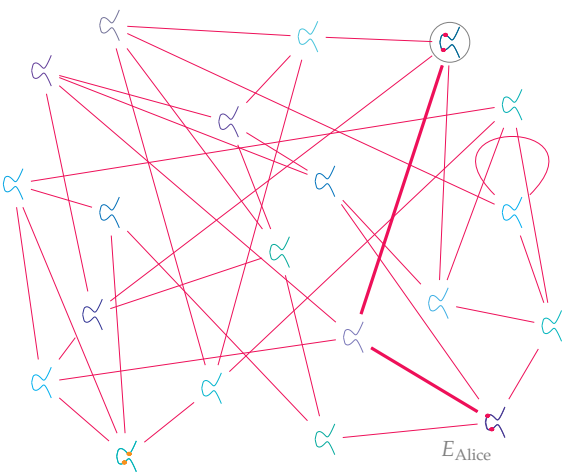
2-isogeny
secret path



3-isogeny
secret path

SIDH KEY EXCHANGE

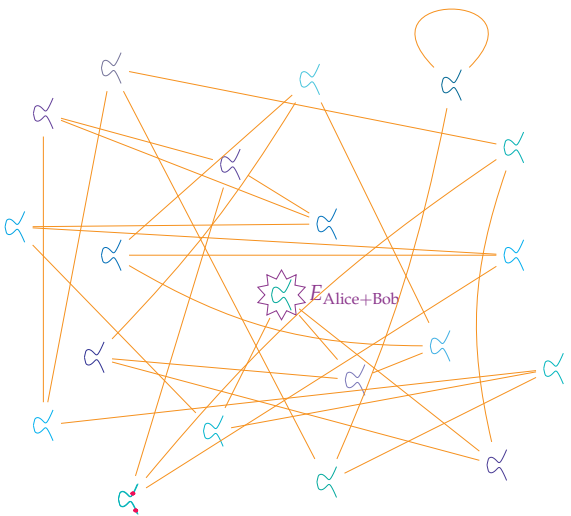




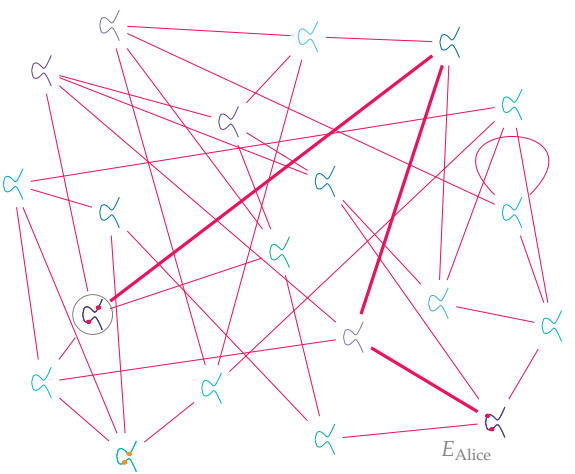
2-isogeny
secret path

3-isogeny
secret path

SIDH KEY EXCHANGE

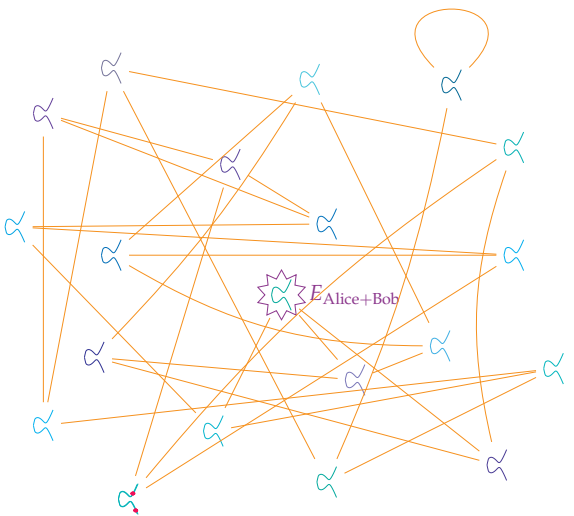


2-isogeny
secret path

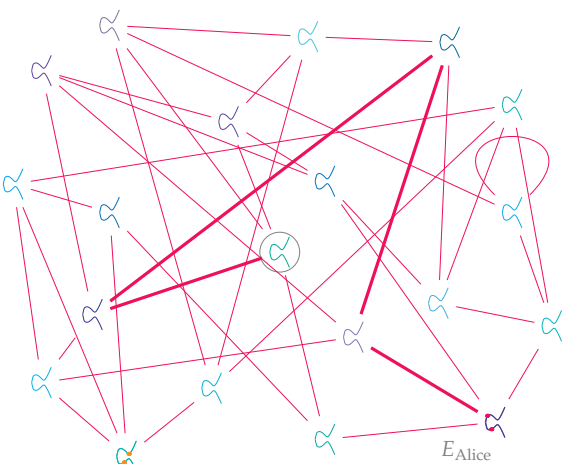


3-isogeny
secret path

SIDH KEY EXCHANGE

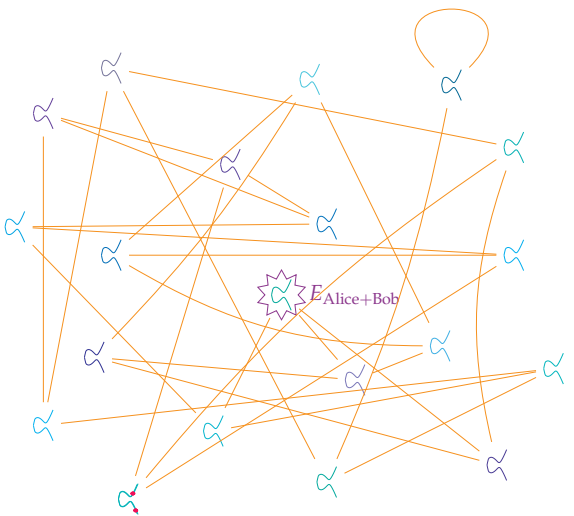


2-isogeny
secret path

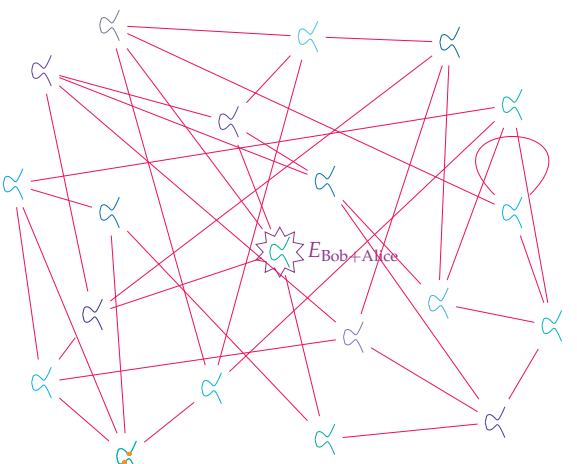


3-isogeny
secret path

SIDH KEY EXCHANGE

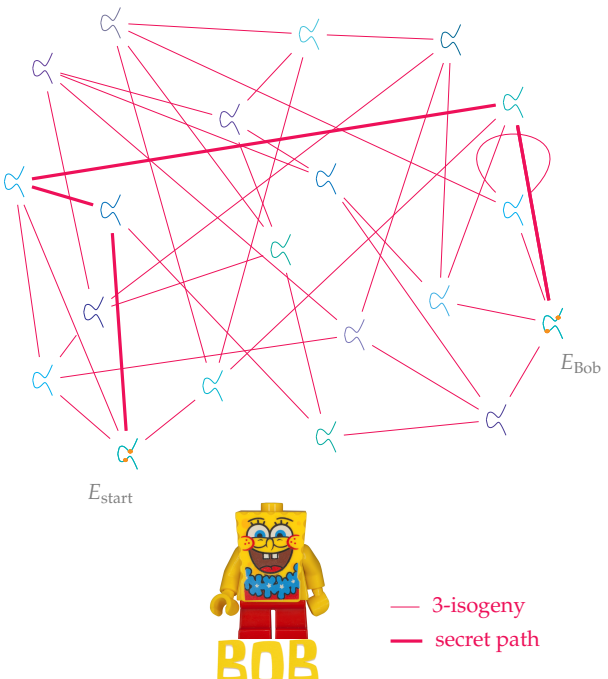


2-isogeny
secret path

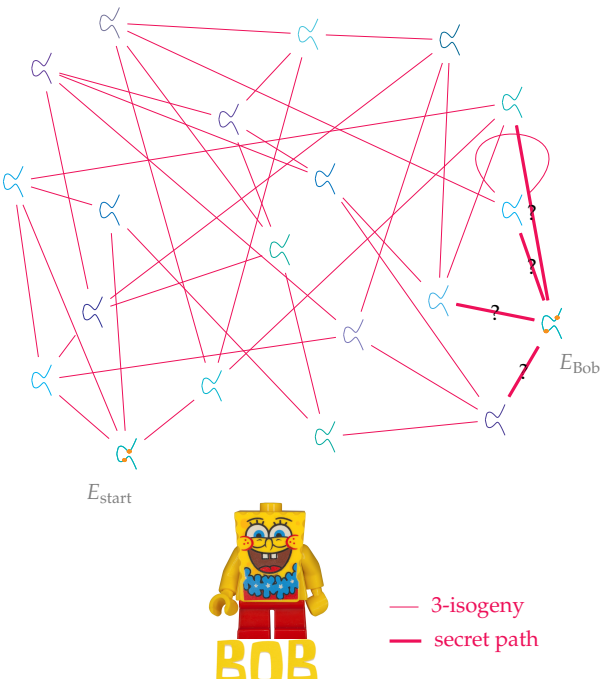


3-isogeny
secret path

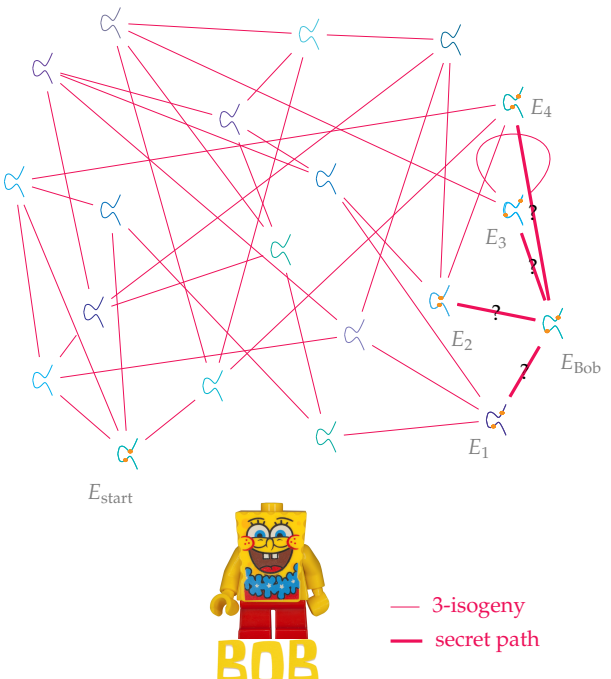
Retrieving Bob's key



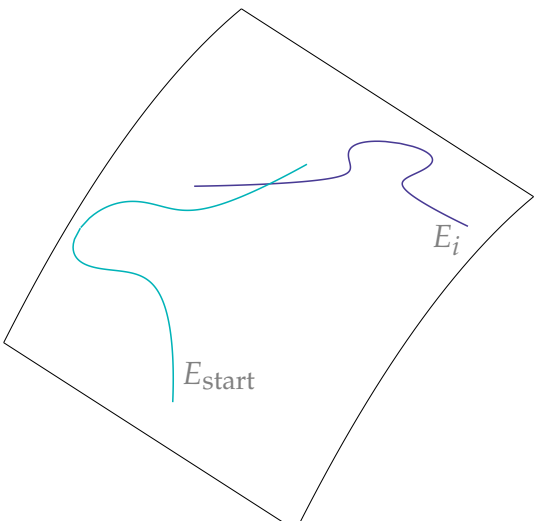
Retrieving Bob's key



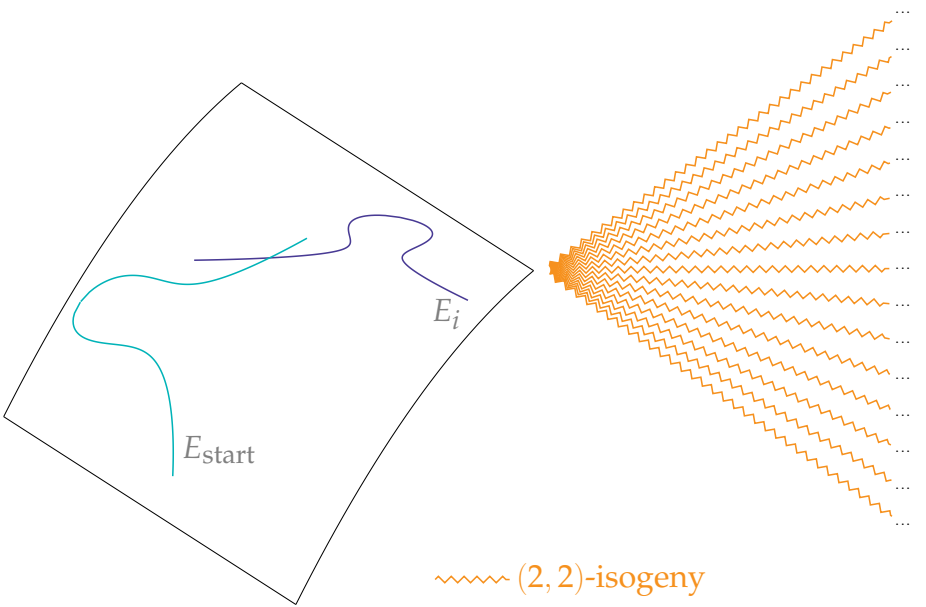
Retrieving Bob's key



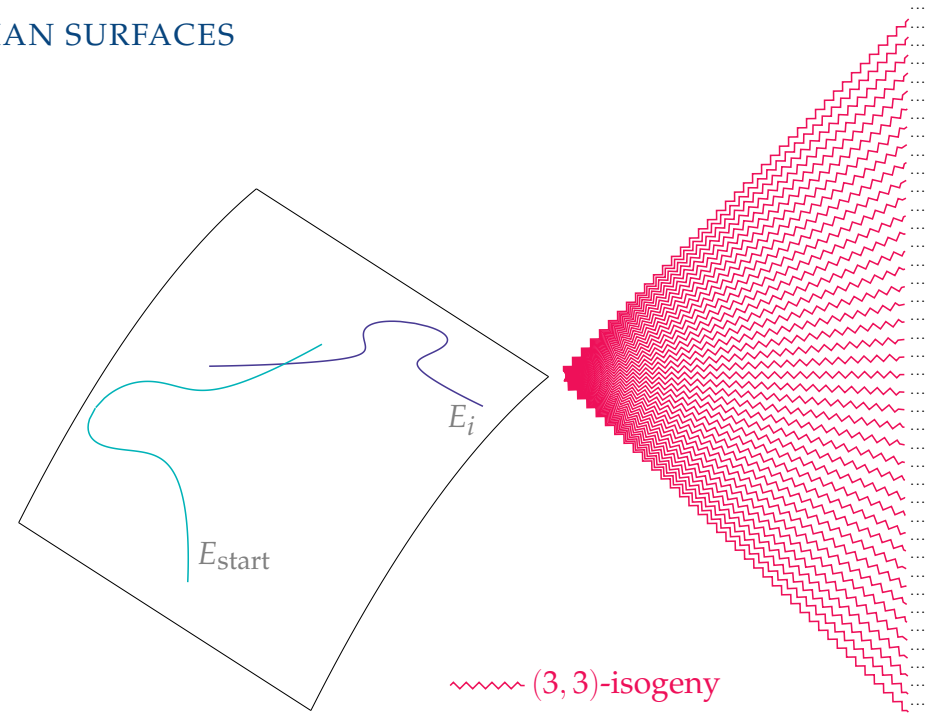
Abelian surfaces



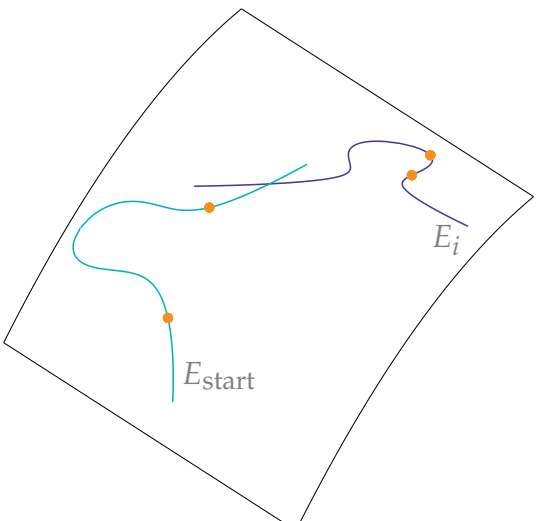
Abelian surfaces



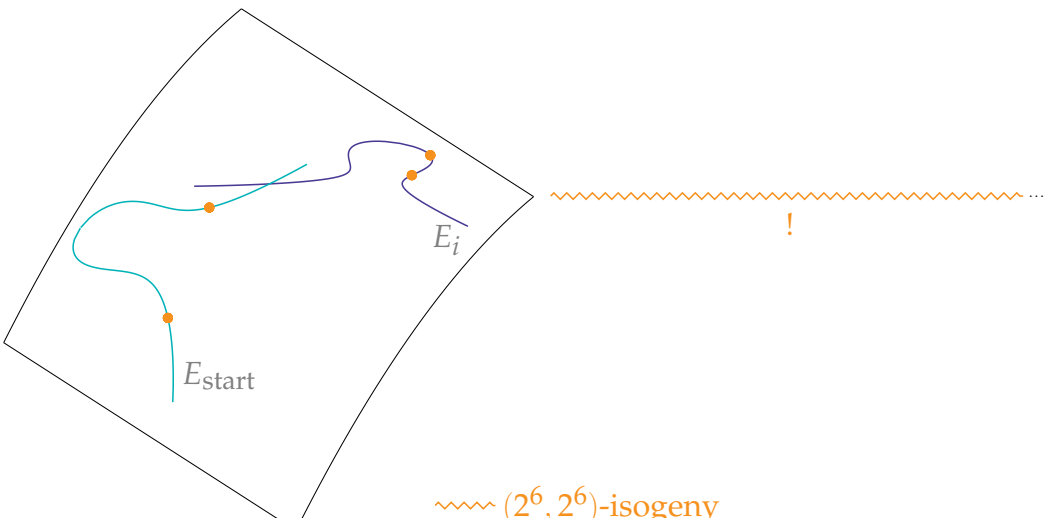
Abelian surfaces



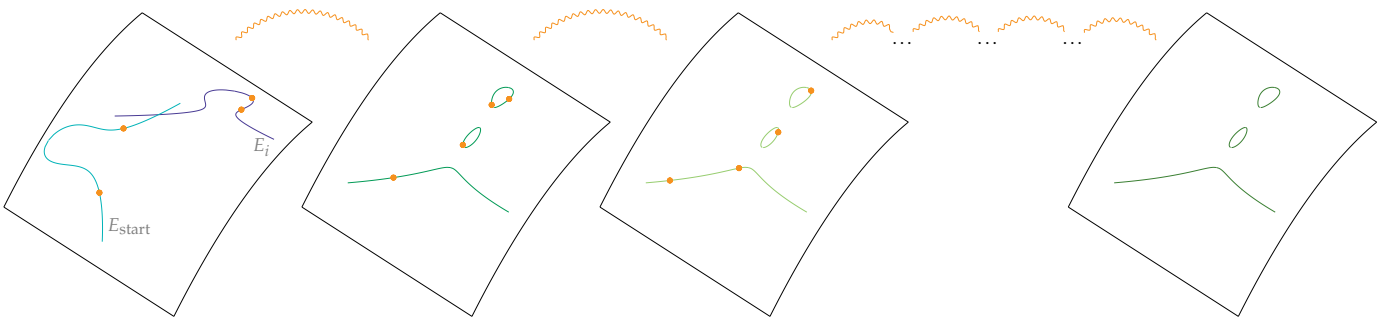
Abelian surfaces



ABELIAN SURFACES



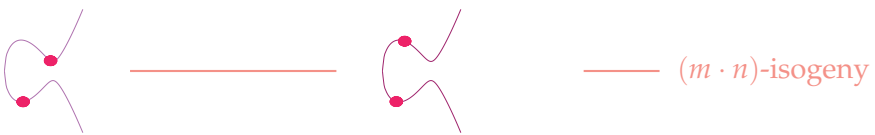
Abelian surfaces from hyperelliptic curves



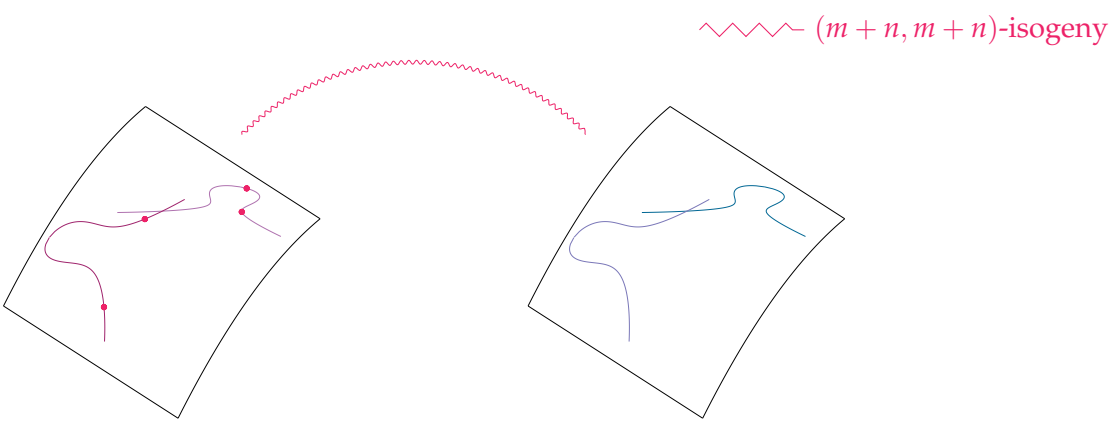
$(2,2)$-isogeny

KANI'S REDUCIBILITY CRITERION (1997)

The one-dimensional isogeny



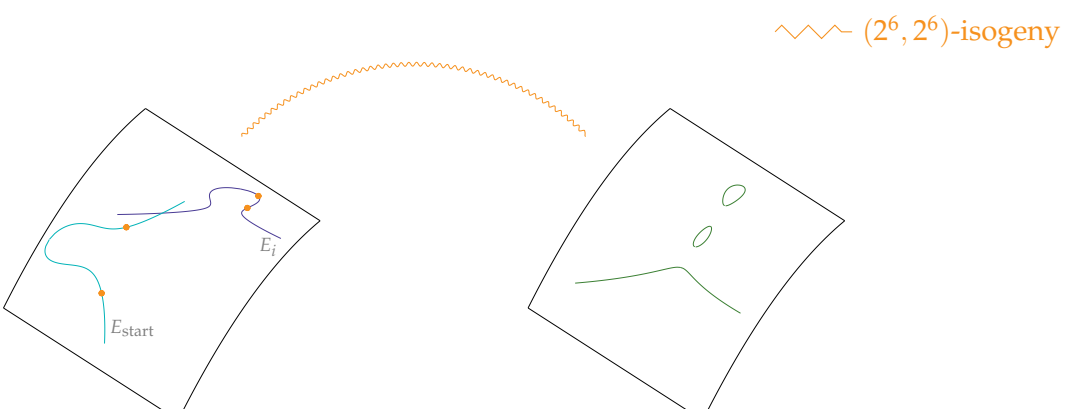
determines the unique two-dimensional isogeny



KANI'S REDUCIBILITY CRITERION (1997)

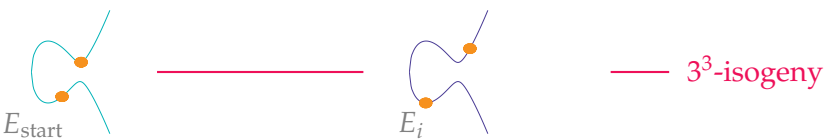
The one-dimensional isogeny

determines the unique two-dimensional isogeny

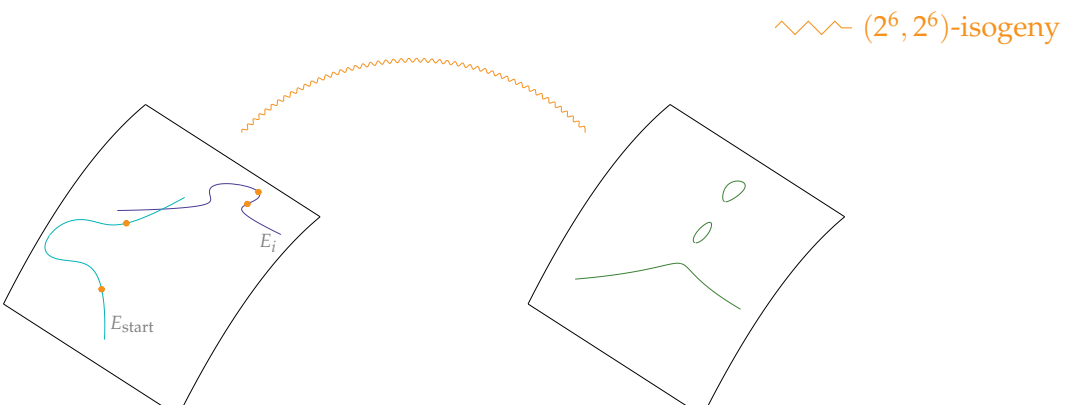


KANI'S REDUCIBILITY CRITERION (1997)

The one-dimensional isogeny

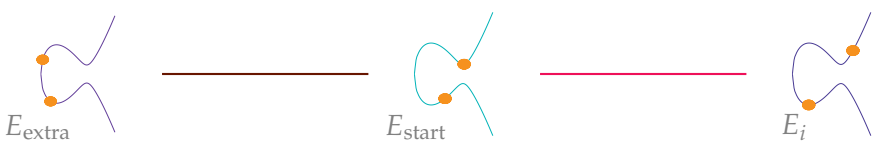


determines the unique two-dimensional isogeny



KANI'S REDUCIBILITY CRITERION (1997)

The one-dimensional isogeny

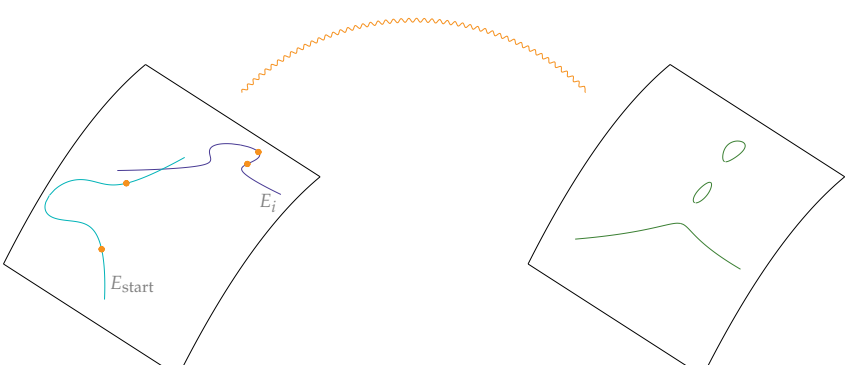


$(2^6 - 3^3)$-isogeny

3^3-isogeny

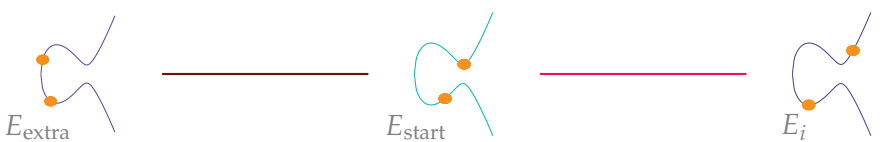
determines the unique two-dimensional isogeny

$(2^6, 2^6)$-isogeny



KANI'S REDUCIBILITY CRITERION (1997)

The one-dimensional isogeny

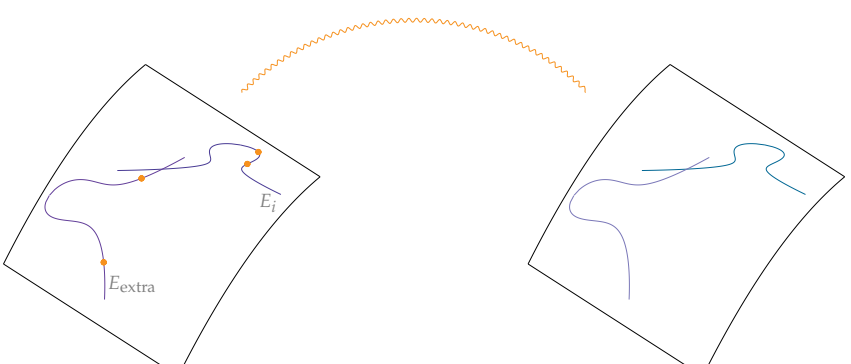


$(2^6 - 3^3)$-isogeny

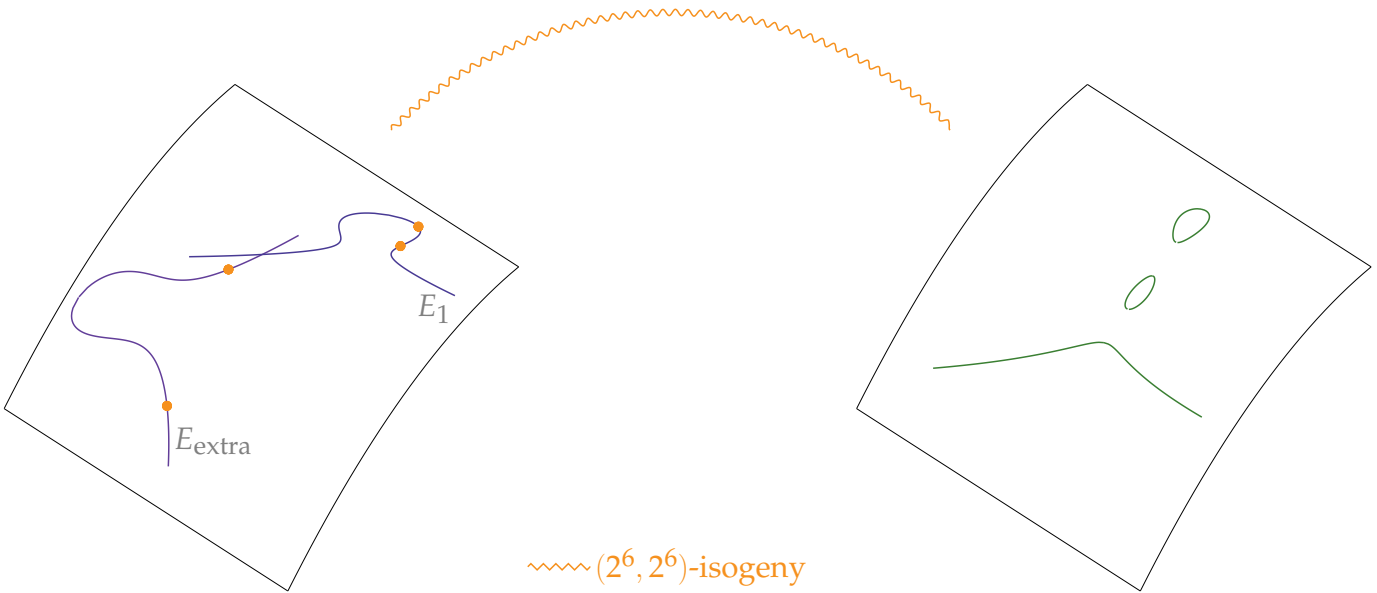
3^3-isogeny

determines the unique two-dimensional isogeny

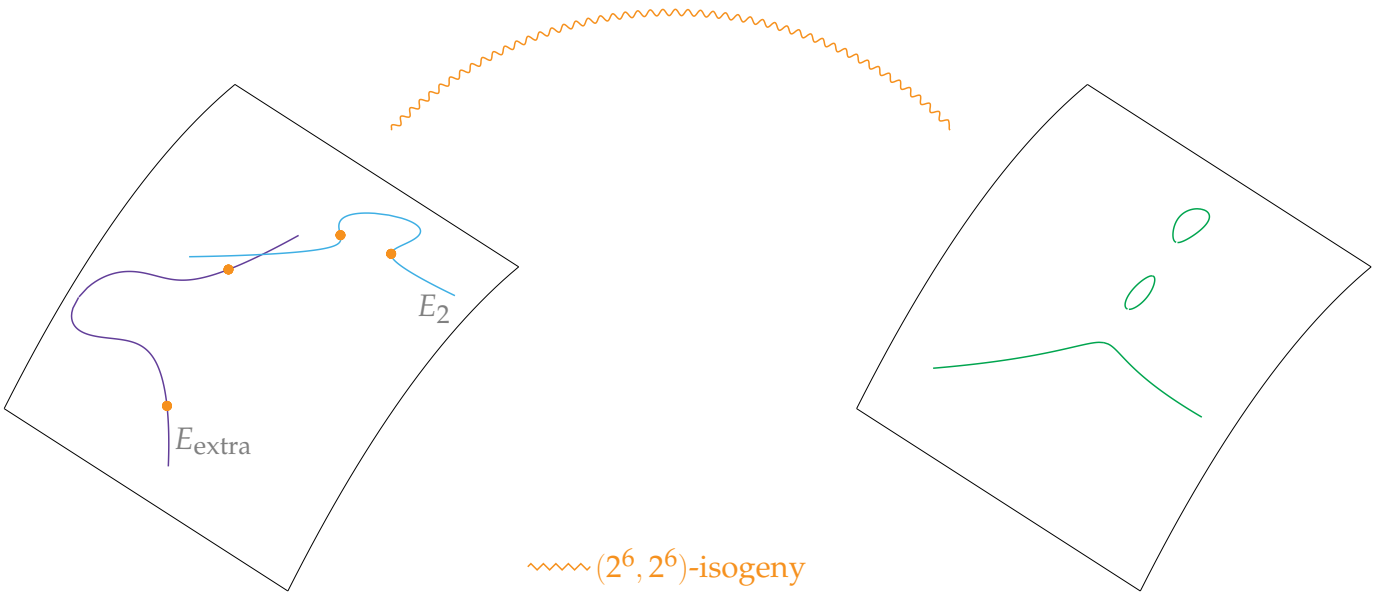
$(2^6, 2^6)$-isogeny



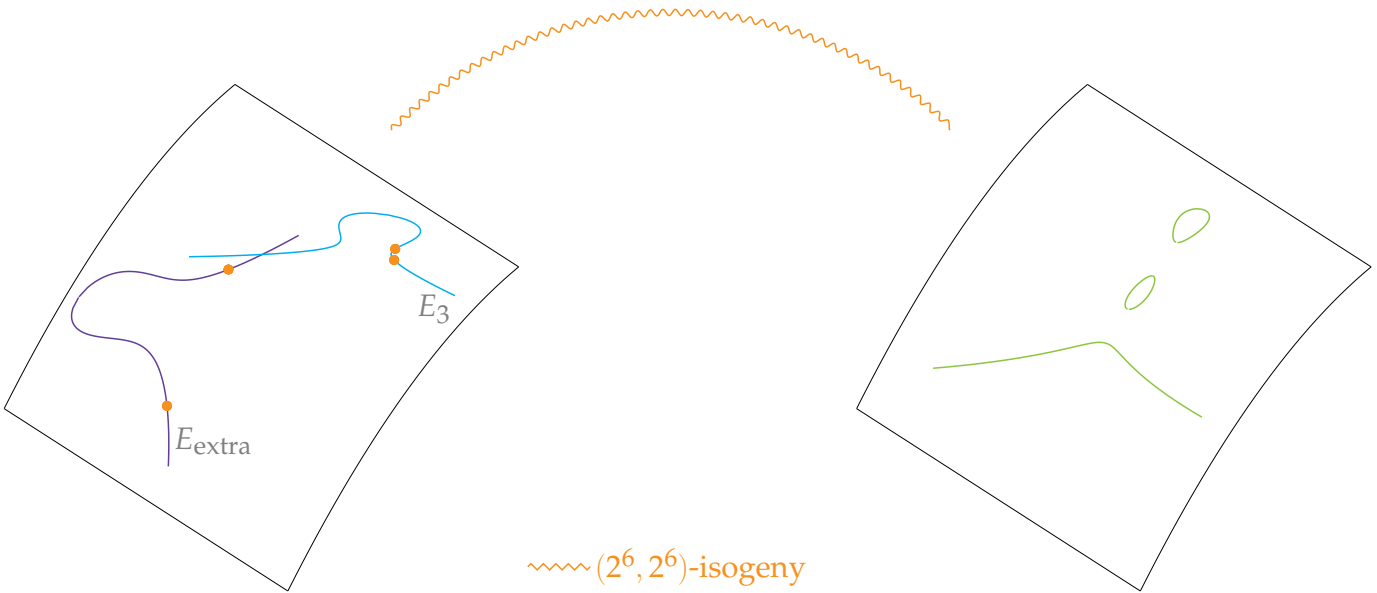
Trial and error



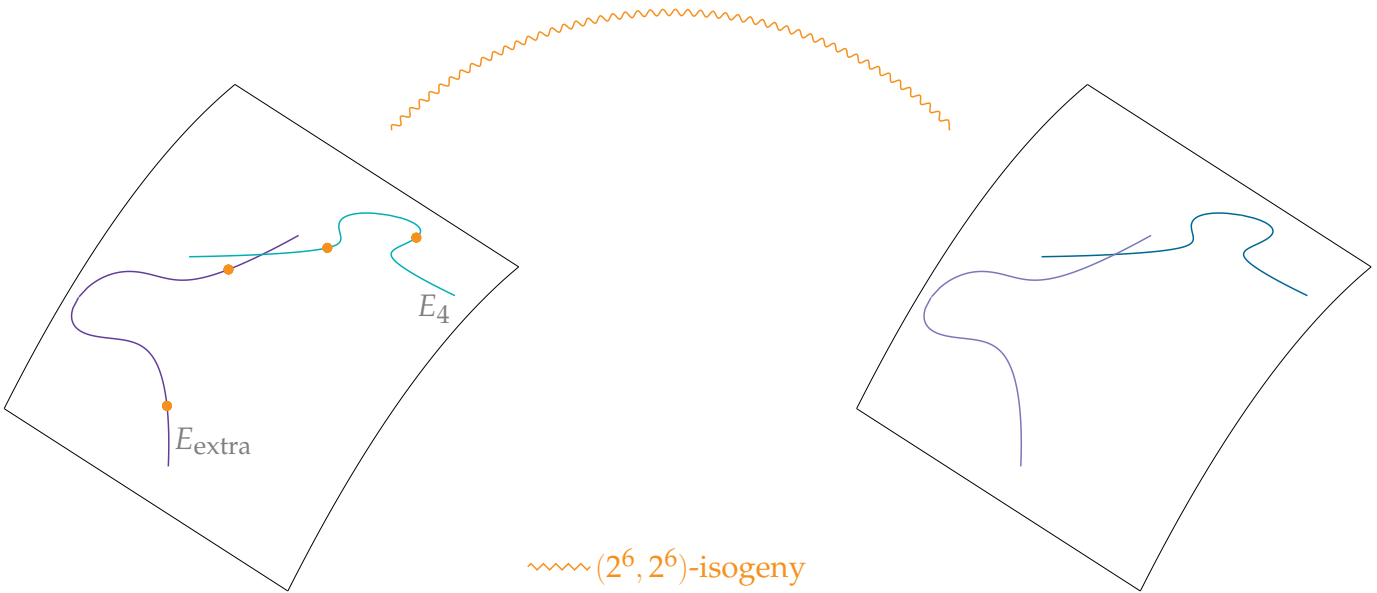
Trial and error



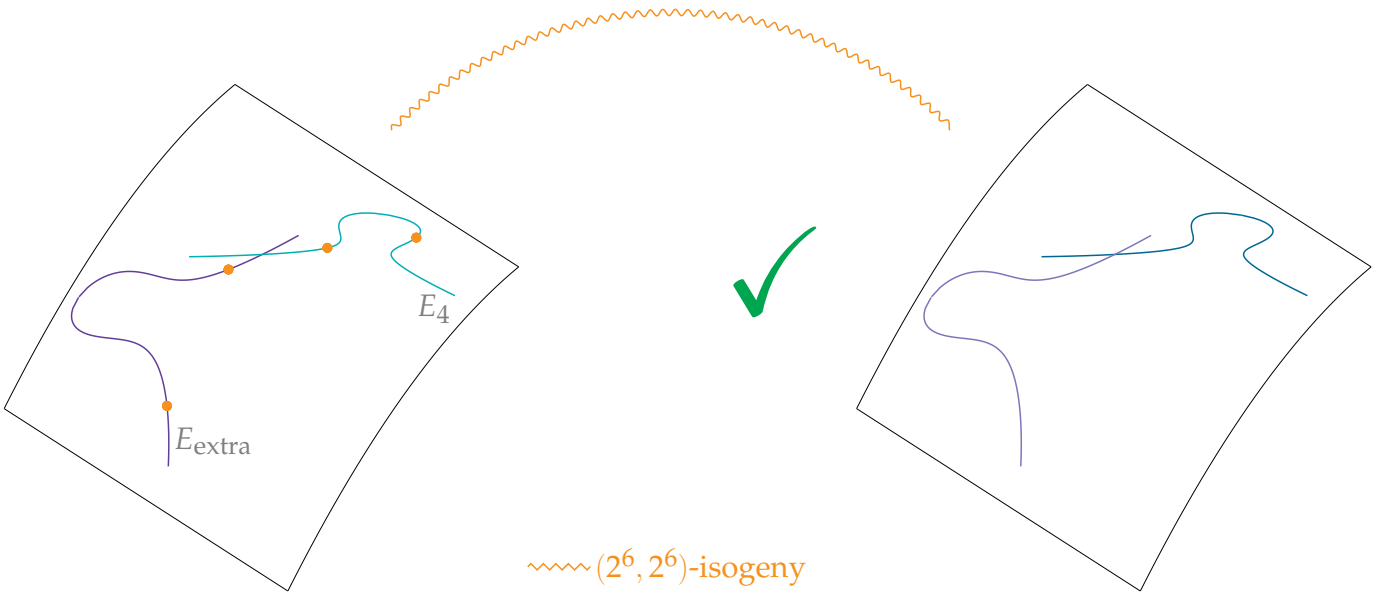
Trial and error



Trial and error



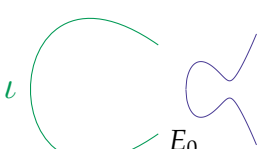
Trial and error



Computing $(2^a - 3^b)$-isogenies in SIKE

- $E_0 : y^2 = x^3 + x$ was used in initial SIKE submission.
  This allows for an easy $(2^a - 3^b)$-isogeny from ι if we write

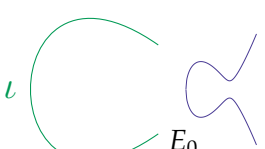
$$2^a - 3^b = (u + 2v\sqrt{-1}) \cdot (u - 2v\sqrt{-1}).$$



Computing $(2^a - 3^b)$-isogenies in SIKE

- $E_0 : y^2 = x^3 + x$ was used in initial SIKE submission.
  This allows for an easy $(2^a - 3^b)$-isogeny from ι if we write

$$2^a - 3^b = (u + 2v\sqrt{-1}) \cdot (u - 2v\sqrt{-1}).$$

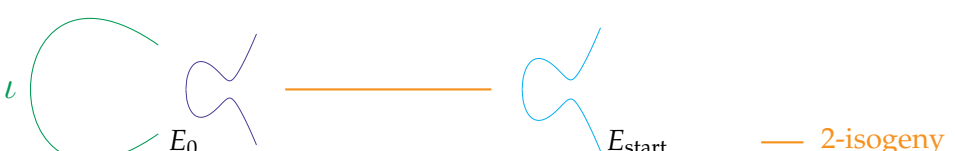


- $E_{\text{start}} : y^2 = x^3 + 6x^2 + x$ was used in later versions of SIKE but similar applies.

Computing $(2^a - 3^b)$-isogenies in SIKE

- $E_0 : y^2 = x^3 + x$ was used in initial SIKE submission.
  This allows for an easy $(2^a - 3^b)$-isogeny from ι if we write

$$2^a - 3^b = (u + 2v\sqrt{-1}) \cdot (u - 2v\sqrt{-1}).$$



- $E_{\text{start}} : y^2 = x^3 + 6x^2 + x$ was used in later versions of SIKE but similar applies.

Computing $(2^a - 3^b)$-isogenies in SIDH

- Can be done if all isogenies from E_{start} to itself are known.

Computing $(2^a - 3^b)$-isogenies in SIDH

- Can be done if all isogenies from E_{start} to itself are known.
- If not: hope $2^a - 3^b$ is smooth.

Computing $(2^a - 3^b)$-isogenies in SIDH

- Can be done if all isogenies from E_{start} to itself are known.
- If not: hope $2^a - 3^b$ is smooth.
- Leeway allows us to find a smooth (positive) expression of the form

$$d \cdot 2^{a-i} - e \cdot 3^{b-j},$$

which leads to a subexponential attack.

TIMINGS

	Quantum security level	Time
$IKEp182	-	55s
$IKEp217	-	85s
SIKEp434	NIST 1	10m
SIKEp503	NIST 2	20m
SIKEp610	NIST 3	55m
SIKEp751	NIST 5	3h15m

Key ingredients for our attack

Requirements:

- degrees of isogenies are fixed and known (i.e. 2^a-isogeny and 3^b-isogeny);
- Alice and Bob exchange extra point images under their respective isogenies.

This attack does *not* apply to other isogeny-based protocols such as CSIDH, SQISign, M(D)-SIDH, etc.

Key ingredients for our attack

Requirements:

- degrees of isogenies are fixed and known (i.e. 2^a-isogeny and 3^b-isogeny);
- Alice and Bob exchange extra point images under their respective isogenies.

This attack does *not* apply to other isogeny-based protocols such as CSIDH, SQISign, M(D)-SIDH, etc.

Blogpost of this talk: